키토큰 사용자 매뉴얼

KeyToken User Manual - 20140112

㈜키페어

www.keypair.co.kr

[Blank Page]

목 차

그 림 목 차

[Blank Page]

I. KeyToken 소개

1. KeyToken 개요

KeyToken은 공인인증서를 안전하게 저장하고 또 안전하게 사용하기 위한 보안 제품으로, 한국인터넷진흥원(KISA)이 KeyToken의 보안토큰에 대한 구현적합성을 평가하고 인증한 제품입니다.

KeyToken 제품은 공인인증서 전용 제품인 KeyToken HSM, microSD 리더기 겸용 제품인 KeyToken MSD, USB 메모리 겸용 제품인 KeyToken USB의 3가지 모델이 있습니다.

2. KeyToken HSM

그림 1의 KeyToken HSM은 그림 2와 같이 보안토큰과 백업영역을 가진 공인인증서 전용 제품입니다.

그림 1. KeyToken HSM의 앞면과 뒷면

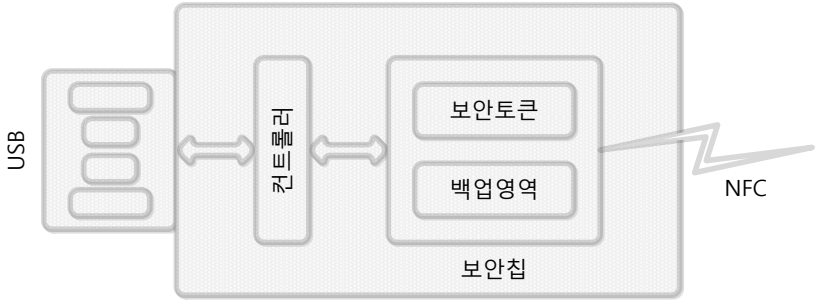

그림 2. KeyToken HSM의 구성도

KeyToken의 보안토큰은 물리적 보안 및 암호연산기능을 가진 보안칩 안에서 구현되어, 현재 공인인증서를 저장하고 사용하는 방법들 중에서 가장 안전합니다.

✧ **KeyTokne의 보안토큰은 공인인증서가 외부로 유출되지 않아 안전합니다.**
이동식 디스크나 하드 디스크에 저장되어 있는 공인인증서는 쉽게 복사될 수 있어, 해킹 등으로 쉽게 유출될 수 있습니다. 하지만, KeyToken의 보안토큰에 저장되어 있는 공인인증서는 보안토큰 내부에서만 사용되며, 이동식 디스크나 하드 디스크로 복사되지 않아서 공인인증서의 외부유출을 원천적으로 방지하여 안전합니다.

✧ **KeyToken의 보안토큰을 사용하여 새로운 공인인증서를 발급받을 수 있습니다.**
금융기관 홈페이지에서 KeyToken의 보안토큰을 사용하여 공인인증서를 새로 발급받으면, 공인인증서의 외부유출이 원천적으로 방지되기 때문에, 공인인증서를 가장 안전하게 사용할 수 있습니다.

✧ **기존의 공인인증서를 KeyToken의 보안토큰으로 복사하여 사용할 수 있습니다.**
이동식 디스크나 하드 디스크에 저장되어 있는 기존의 공인인증서는 KeyToken의 보안토큰으로 복사하여 안전하게 사용할 수 있습니다. 이때 기존의 공인인증서는 KeyToken의 백업영역과 같은 안전한 곳에 백업하여 보관하시기 바랍니다.

✧ **KeyToken의 보안토큰은 최대 6개의 공인인증서를 저장할 수 있습니다.**
KeyToken의 보안토큰은 은행용/증권용/범용/법인용 등 최대 6개의 공인인증서를 저장하여 사용할 수 있습니다.

✧ **NFC 스마트폰에서 KeyToken의 보안토큰을 사용할 수 있도록 준비 중입니다.**
KeyToken의 보안토큰은 PC에서 USB로 연결하여 은행, 증권사 등의 홈페이지에서 바로 사용가능하며, NFC 스마트폰에서도 사용할 수 있도록 준비 중입니다. 현재, 스마트폰의 금융앱이 KeyToken의 보안토큰과 NFC로 통신하는 기능을 협의 중에 있으며, 기능이 추가되기 전까지는 KeyToken의 백업영역 기능을 사용하여 현재의 방식보다 안전하게 스마트폰에서 공인인증서를 사용할 수 있습니다.

KeyToken의 백업영역도 물리적 보안 및 암호연산기능을 가진 보안칩 안에서 구현되어, 현재 공인인증서를 백업하는 방법들 중에서 가장 안전합니다.

✧ **KeyToken의 백업영역은 하나의 공인인증서를 백업할 수 있습니다.**

KeyToken의 백업영역은 하나의 공인인증서를 백업하여 보관할 수 있습니다.

✧ **KeyToken의 백업영역에 보관중인 공인인증서는 이동식 디스크로 복사할 수 있습니다.**

은행, 증권사, 보험사, 신용카드사, 전자민원, 국세청 등 대부분의 금융 및 공공기관 홈페이지에서 KeyToken의 보안토큰을 사용할 수 있습니다만, 드물게 보안토큰을 지원하지 않는 사이트들이 존재합니다. 이 경우, KeyToken의 백업영역에 보관되어 있는 공인인증서를 이동식 디스크로 복사하여 사용할 수 있습니다.

✧ **KeyToken의 백업영역에 보관중인 공인인증서는 NFC 스마트폰으로 복사할 수 있습니다.**

KeyToken의 백업영역에 보관되어 있는 공인인증서를 NFC 스마트폰으로 복사하여, 현재의 방식보다 안전하게 공인인증서를 사용할 수 있습니다. 자세한 내용은 'KeyToken App Manual'을 참조하시기 바랍니다.

KeyToken의 보안칩은 자동잠김기능과 초기화기능 등을 제공하여 공인인증서를 안전하게 관리합니다.

✧ **KeyToken의 보안칩은 자동잠김기능이 있어, 분실시에도 안전합니다.**

KeyToken의 보안칩은 8자이상 16자이하의 비밀번호를 사용합니다. 이 비밀번호가 연속으로 5회이상 틀리면, KeyToken의 보안칩은 자동으로 잠겨서 보안토큰과 백업영역을 더 이상 사용할 수 없도록 합니다. 타인이 8자이상의 비밀번호를 5회안에 맞추는 것은 확률적으로 거의 불가능하므로, KeyToken을 분실하더라도 KeyToken 안의 공인인증서는 사실상 안전합니다.

✧ **KeyToken의 보안칩은 초기화기능이 있어, 본인이 KeyToken 비밀번호를 잊어버린 경우에도 KeyToken 제품은 다시 사용할 수 있습니다.**

KeyToken의 보안칩은 본인이 KeyToken 비밀번호를 잊어버린 경우에도 초기화하여 다시 사용할 수 있습니다. 다만, 초기화될 때 KeyToken 비밀번호와 보안토큰, 백업영역 안의 모든 데이터가 완전히 삭제되므로, KeyToken 비밀번호를 새로 설정해야 하고 공인인증서도 새로 발급받거나 다시 복사해 넣어야 합니다.

3. KeyToken MSD

그림 3의 KeyToken MSD는 그림 4와 같이 보안토큰, 백업영역, microSD 리더기를 가진 제품입니다.

그림 3. KeyToken MSD의 앞면과 뒷면

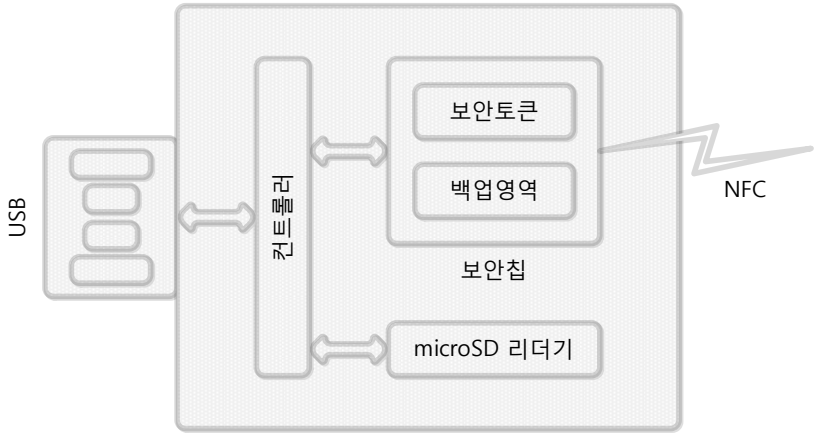

그림 4. KeyToken MSD의 구성도

KeyToken MSD에서 보안토큰, 백업영역, 보안칩에 대한 기능은 KeyToken HSM에서의 기능과 동일합니다. KeyToken MSD는 KeyToken HSM과 PC용 microSD 리더기가 결합된 제품입니다. (microSD 메모리는 별매품입니다.)

✧ **KeyToken MSD에 microSD를 넣은 후 이동식 디스크로 사용할 수 있습니다.**

그림 3의 오른쪽 그림과 같이 KeyToken MSD 뒷면의 뚜껑을 연 후, microSD를 넣고 뺄 수 있습니다.

✧ **사용자가 원하는 성능과 용량의 microSD/SDHC/SDXC를 사용할 수 있습니다.**

KeyToken의 microSD 리더기는 최대 20MB/s의 전송속도와 최대 64GB의 용량을 지원합니다.

4. KeyToken USB

그림 5의 KeyToken USB는 그림 6과 같이 보안토큰, 백업영역, USB 메모리를 가진 제품입니다.

그림 5. KeyToken USB의 앞면과 뒷면

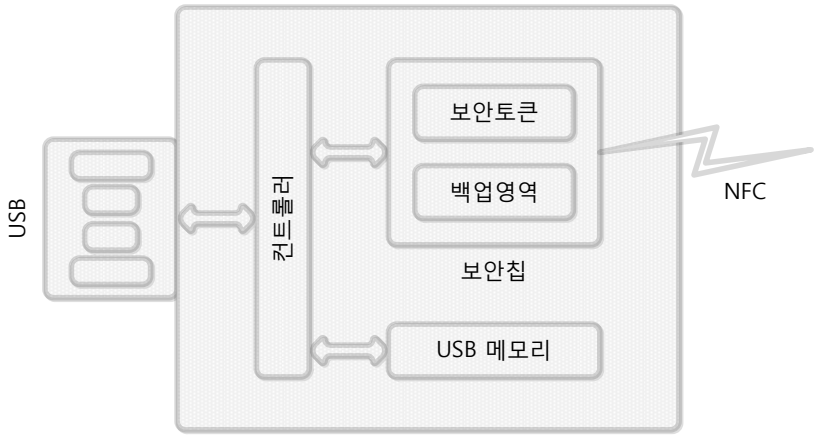

그림 6. KeyToken USB의 구성도

KeyToken USB에서 보안토큰, 백업영역, 보안칩에 대한 기능은 KeyToken HSM에서의 기능과 동일합니다. KeyToken USB는 KeyToken HSM과 PC용 USB 메모리가 결합된 제품입니다.

✧ **다양한 용량의 USB 메모리를 사용할 수 있습니다.**

KeyToken의 USB 메모리는 8GB의 경우 최대 18MB/s의 쓰기, 최대 20MB/s의 읽기 성능을 가집니다. 용량은 8 / 16 / 32 / 64GB 제품이 있습니다.

※ 키페어는 제품에 저장된 데이터의 손실에 대한 복구나 배상 책임을 지지 않습니다. 데이터가 손실되지 않도록 반드시 백업하면서 사용하시기 바랍니다.

5. KeyToken 사용환경

✧ **PC**

인터페이스 : USB 1.1 / 2.0

운영체제 : Windows 8 (32/64-bit), Windows 7 (32/64-bit), Windows Vista (32/64-bit), Windows XP (32-bit)

✧ **스마트폰**

인터페이스 : NFC

운영체제 : 안드로이드 v2.3.6 (진저브레드) 이상

II. KeyToken 구동 프로그램

KeyToken을 PC에서 사용하기 위해서는, 먼저 PC에 구동 프로그램을 설치해야 합니다.

1. 구동 프로그램 다운로드

KeyToken 구동 프로그램은 키페어에서 제공하는 KeyTokenSetup.exe 파일을 실행하면 설치됩니다. KeyTokenSetup.exe 파일은 아래의 방법으로 구할 수 있습니다.

✧ **microSD를 내장한 KeyToken MSD 제품 또는 KeyToken USB 제품에는 미리 저장되어 있습니다.**

microSD를 내장한 KeyToken MSD 제품은 microSD에, KeyToken USB 제품은 USB 메모리에, KeyTokenSetup.exe 파일이 미리 저장되어 있습니다.

✧ **키페어 홈페이지에서 다운로드 받을 수 있습니다.**

웹 브라우저에서 아래의 주소를 직접 입력하여 키페어의 홈페이지로 접속한 후, 그림 7과 같이 다운로드 페이지로 이동하여 'KeyToken 구동 프로그램' 설치파일을 다운로드 받을 수 있습니다.

http://www.keypair.co.kr

그림 7. 키페어 홈페이지의 다운로드 페이지

2. 구동 프로그램 설치

KeyToken은 PC에서 사용되기 전에, 반드시 PC에 KeyToken 구동 프로그램이 설치되어 있어야 합니다.

이 절에서는 KeyToken HSM에 대한 구동 프로그램을, Windows 7의 Internet Explorer 9로 키페어 홈페이지에서 다운로드 받은 후, 설치하는 과정을 예를 들어서 설명합니다. 기본적으로 Windows 8, Windows Vista, Windows XP에서도 동일한 과정으로 설치됩니다. 다만, 설치에 앞서 운영체제를 최신 상태로 업데이트하시기를 권장합니다.

1 그림 8과 같이 키페어 홈페이지의 다운로드 페이지에서 해당 제품의 '실행파일 다운로드' 버튼을 누릅니다.

그림 8. 실행파일 다운로드

※ microSD를 내장한 KeyToken MSD 제품 또는 KeyToken USB 제품은 미리 저장되어 있는 KeyTokenSetup.exe 파일을 사용하여 바로 [3] 단계를 진행하시면 됩니다.

2 그림 9 화면에서 '열기'를 선택합니다.

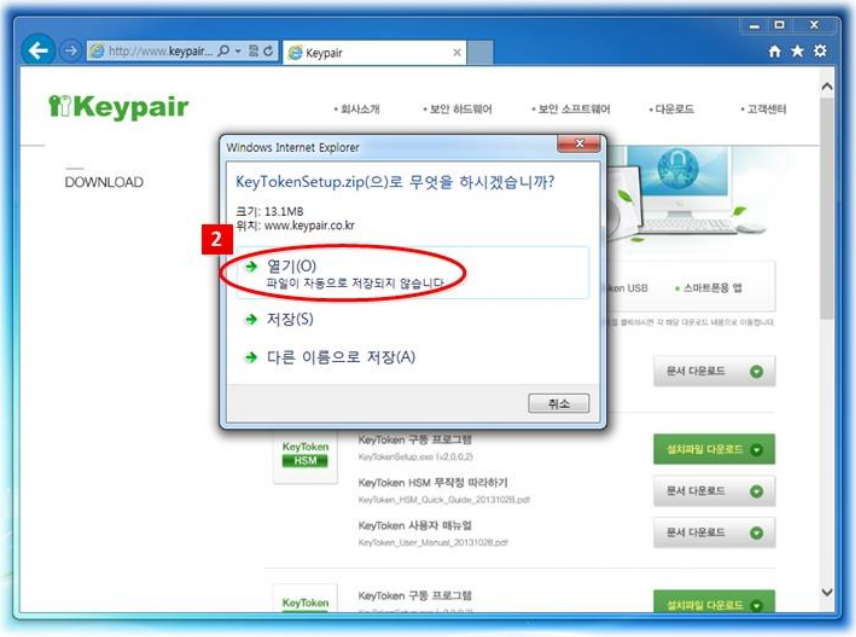

그림 9. KeyTokenSetup.zip 파일 열기

3 그림 10 화면에서 KeyTokenSetup.exe 파일을 더블클릭하여 실행시킵니다.

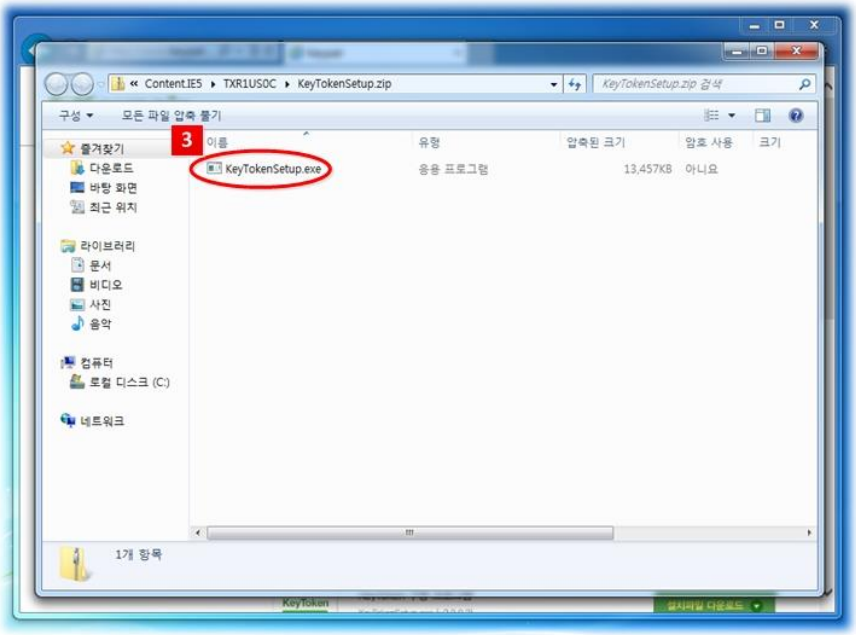

그림 10. KeyTokenSetup.exe 파일 실행하기

※ 그림 10에서, KeyTokenSetup.exe 파일은 운영체제의 환경설정에 따라 'KeyToken Setup'으로 표시될 수 있습니다.

※ KeyTokenSetup.exe 파일은 기능 향상을 위하여 수시로 변경될 수 있습니다. 이때, '클라우드 평판 기반 실행 차단' 기능을 가진 V3와 같은, 사용자 평가 기반의 백신 프로그램은 변경된 KeyTokenSetup.exe 파일 및 설치되는 실행 파일들을 새로운 프로그램으로 인식하여, 충분한 사용자 평가가 이루어지기 전까지 보안 경고를 표시할 수 있습니다.

※ 또한, 운영체제 사용자 계정의 권한에 따라 그림 11과 같은 화면의 확인 메시지가 표시될 수 있습니다.

※ KeyTokenSetup.exe 파일 및 설치되는 실행 파일들에 대한 보안성은 당사에서 충분히 검증한 후 공개하므로, 안심하시고 실행을 허용하시면 됩니다.

3-1 그림 11과 같은 화면이 나타날 경우, '예' 버튼을 누릅니다.

그림 11. 실행 허용 선택하기

※ KeyTokenSetup.exe 파일을 실행하기 위해서는 윈도우 시스템에 'Microsoft .NET Framework 4.0 Client'가 설치되어 있어야 합니다. 윈도우 시스템이 Windows XP 이거나 Windows Vista 이상이라도 최신 업데이트가 적용되어 있지 않다면, 아래의 [3-2] ~ [3-4] 단계를 진행하시어 'Microsoft .NET Framework 4.0 Client'를 설치해야 합니다. 설치 시간은 PC 성능과 네트워크 사정에 따라서 수분에서 수십분이 소요됩니다.

3-2 그림 12 화면에서 '설치' 버튼을 눌러, 'Microsoft .NET Framework 4.0 Client'의 설치를 시작합니다.

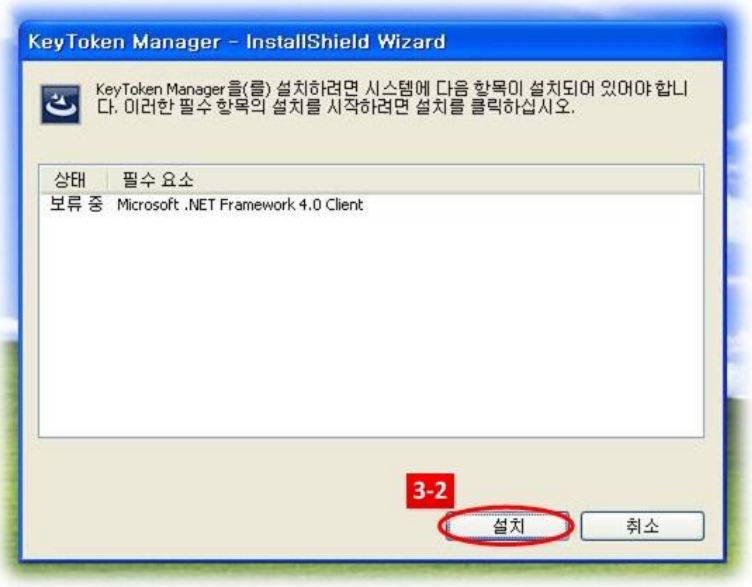

그림 12. Microsoft .NET Framework 4.0 Client 설치 시작

3-3 그림 13 화면에서 다운로드가 완료될 때까지 기다립니다. 네트워크 사정에 따라서 수분에서 수십분이 걸릴 수 있습니다.

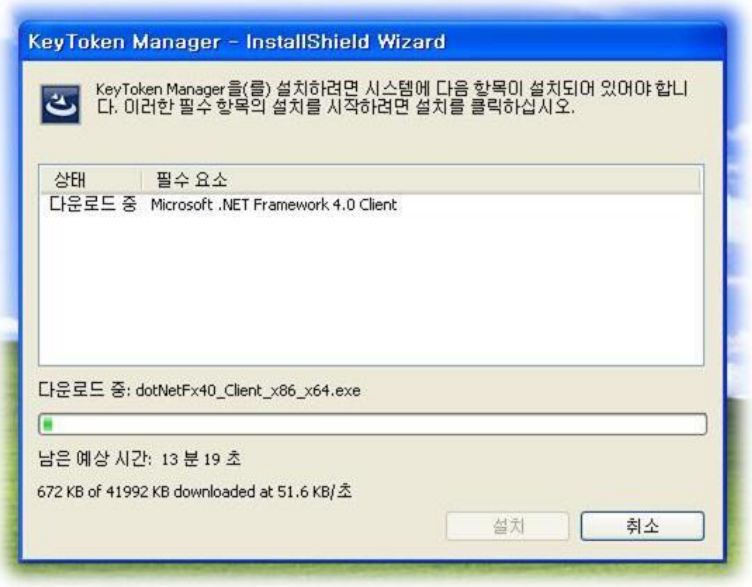

그림 13. Microsoft .NET Framework 4.0 Client 다운로드 중

3-4 그림 14 화면에서 설치가 완료될 때까지 기다립니다. PC 성능에 따라서 수분에서 수십분이 걸릴 수 있습니다.

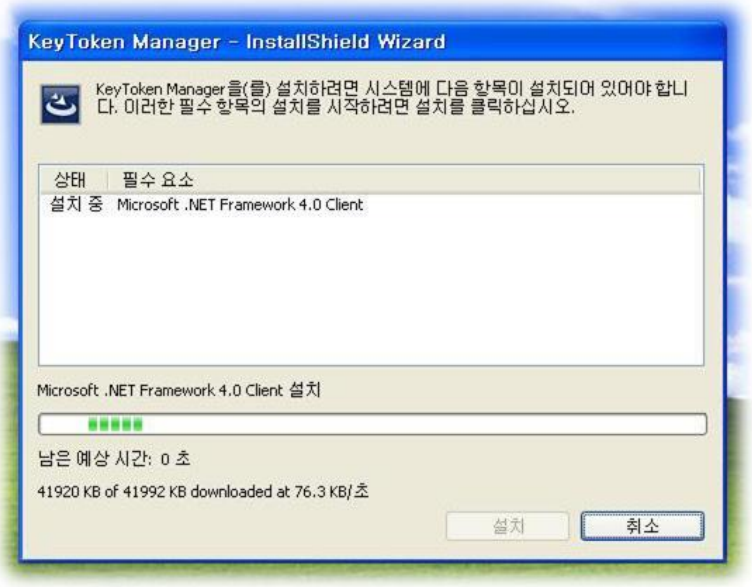

그림 14. Microsoft .NET Framework 4.0 Client 설치 중

4 그림 15 화면에서 '다음' 버튼을 눌러, KeyToken Manager의 설치를 시작합니다.

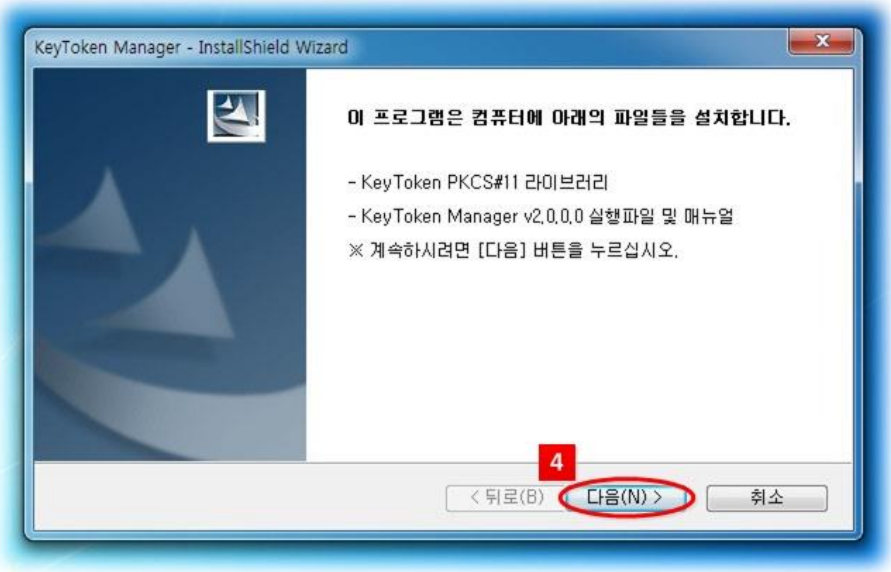

그림 15. KeyToken Manager 설치 시작

5 그림 16 화면이 나타나면 기다립니다.

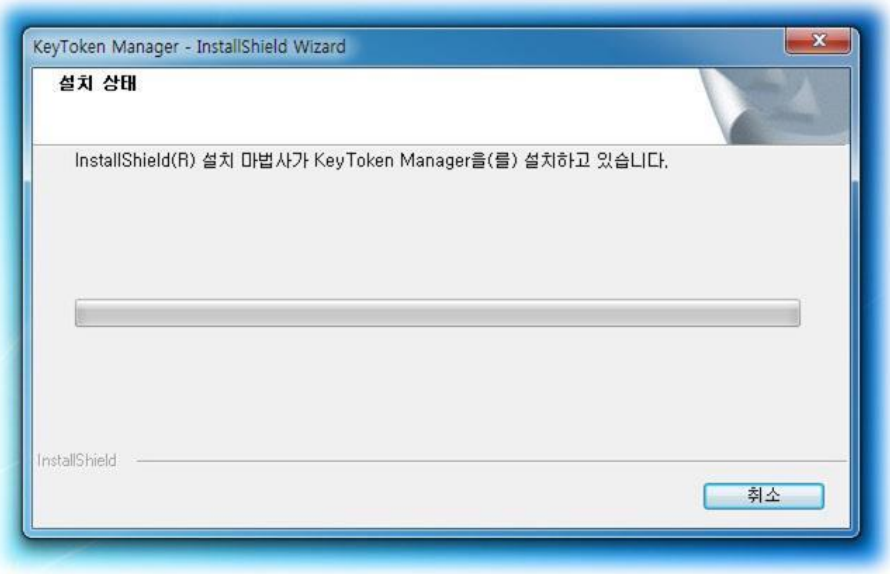

그림 16. KeyToken Manager 설치 진행중

6 PC의 USB포트에 KeyToken이 연결되어 있지 않으면, 그림 17 화면이 나타납니다. PC의 USB포트에 KeyToken을 연결하십시오.

그림 17. KeyToken 찾기

7 PC의 USB포트에 연결된 KeyToken이 초기화되어 있지 않으면, 그림 18 화면이 나타납니다. KeyToken 비밀번호 등 초기화에 필요한 정보를 입력합니다.

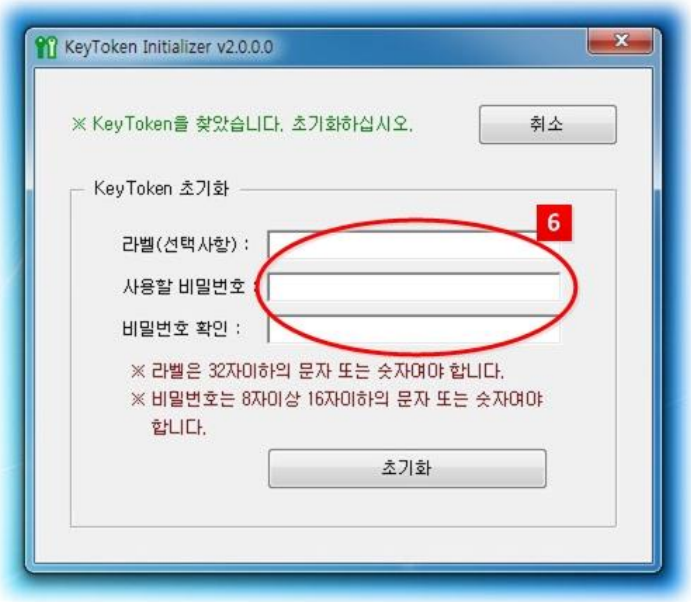

그림 18. KeyToken 초기화 정보 입력

8 그림 19 화면에서 '초기화' 버튼을 눌러, KeyToken을 초기화합니다.

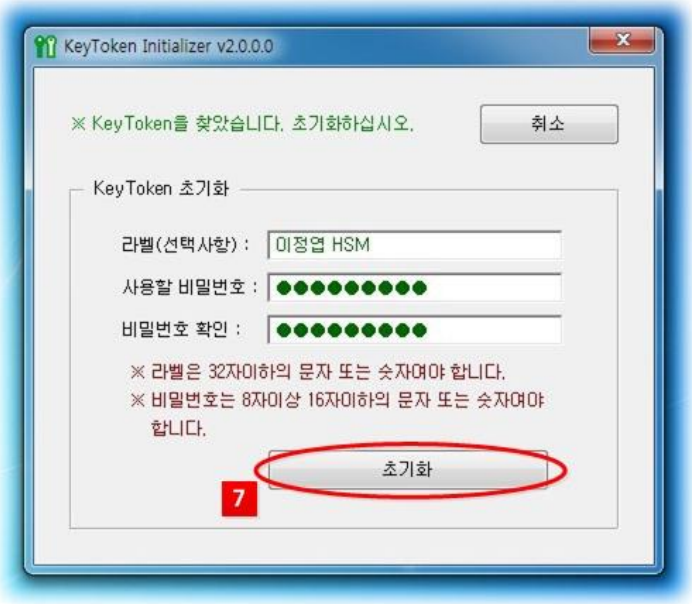

그림 19. KeyToken 초기화 시작

9 그림 20 화면에서 '확인' 버튼을 눌러, KeyToken 초기화를 완료합니다.

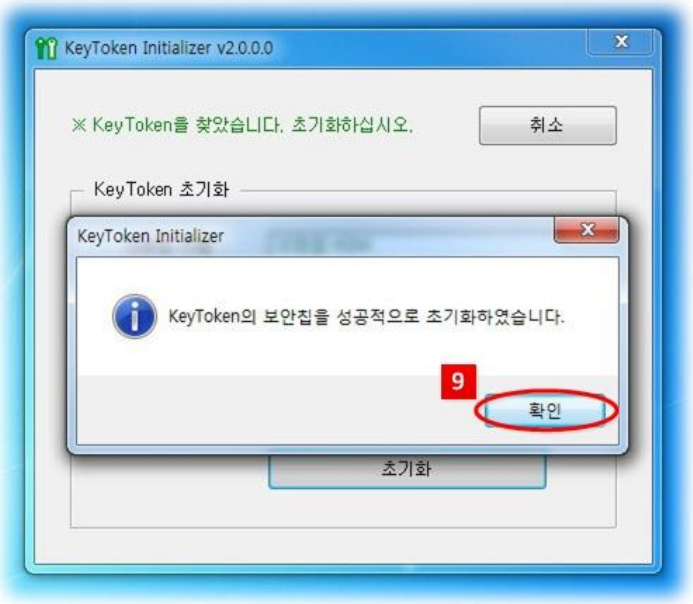

그림 20. KeyToken 초기화 완료

10 그림 21 화면에서 '완료' 버튼을 눌러, KeyToken Manager의 설치를 완료합니다.

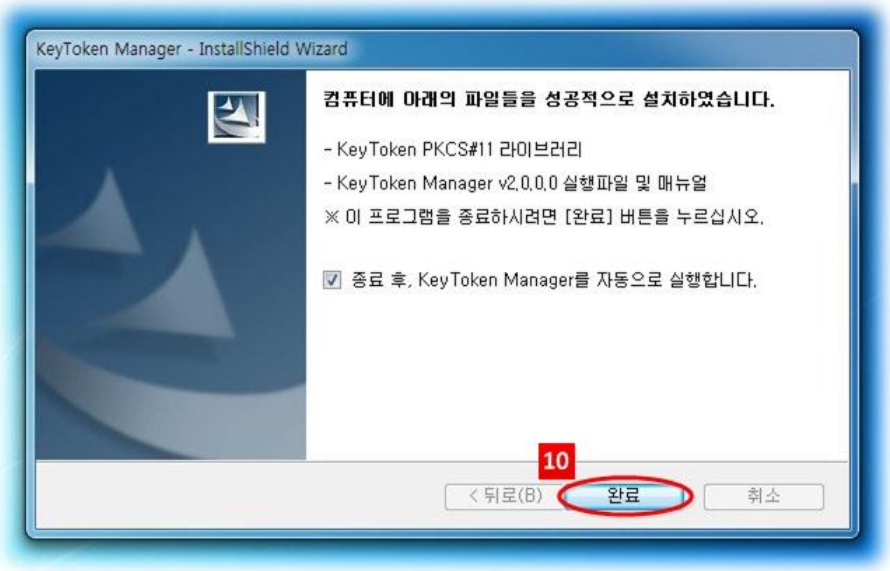

그림 21. KeyToken Manager 설치 완료

3. 구동 프로그램 삭제

이 절에서는 Windows 7에서 설치된 KeyToken 구동 프로그램을 삭제하는 과정을 예를 들어서 설명합니다. 기본적으로 Windows 8, Windows Vista, Windows XP에서도 동일한 과정으로 삭제합니다.

1 Ⅱ장 2절의 '구동 프로그램 설치'에서 [1], [2], [3] 단계를 실행합니다.

※ 윈도우의 제어판에서 '프로그램 제거'를 선택한 후 'KeyToken Manager'를 찾아서 '제거'를 선택하셔도 됩니다.

2 그림 22 화면에서 '다음' 버튼을 눌러, KeyToken Manager의 삭제를 시작합니다.

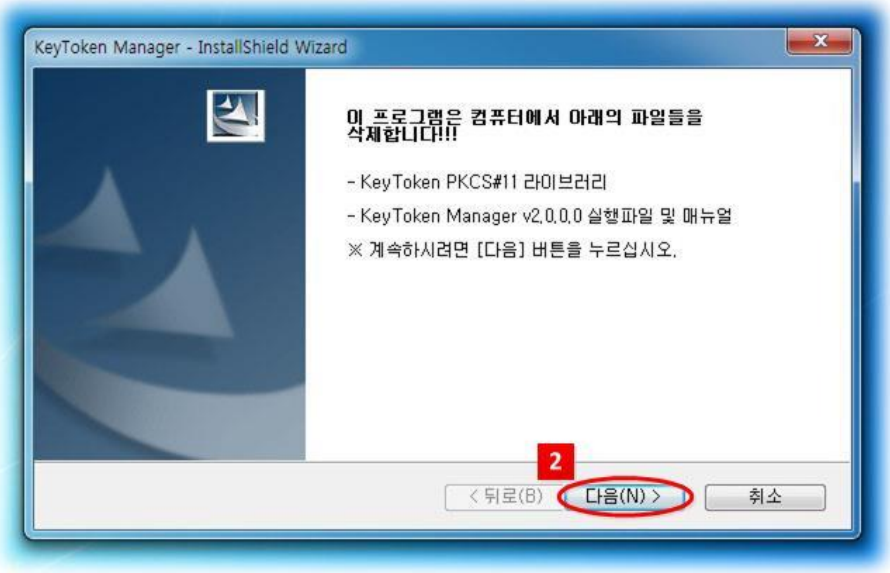

그림 22. KeyToken Manager 삭제 시작

3 그림 23 화면이 나타나면 기다립니다.

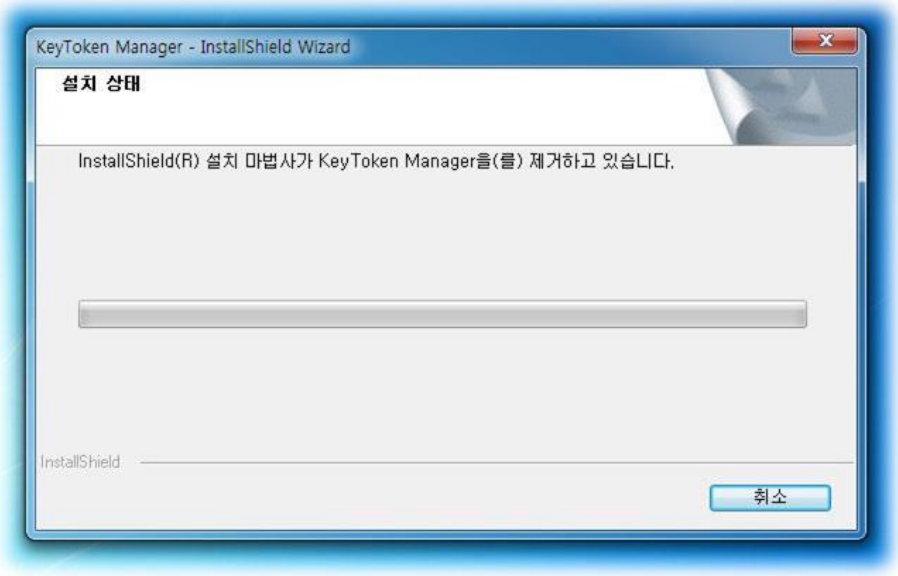

그림 23. KeyToken Manager 삭제 진행중

4 그림 24 화면에서 '완료' 버튼을 눌러, KeyToken Manager의 삭제를 완료합니다.

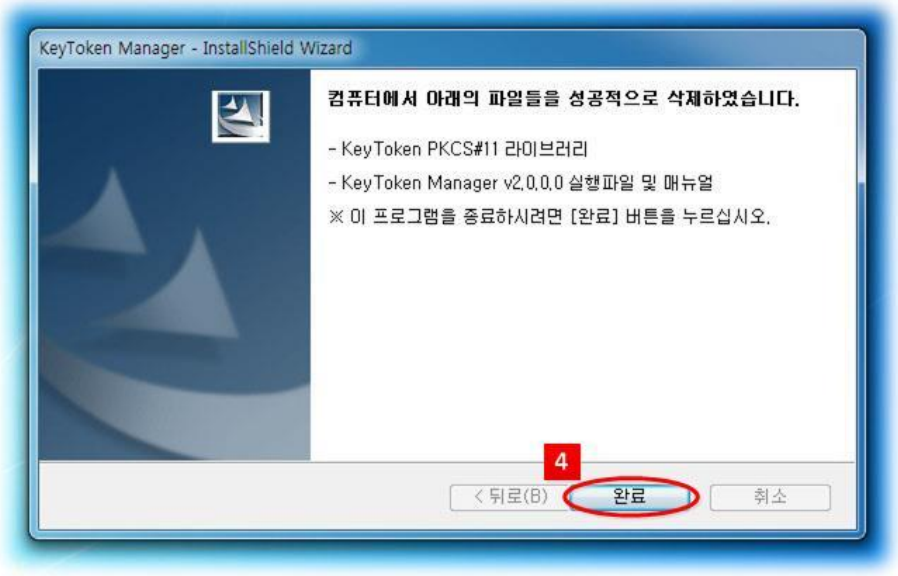

그림 24. KeyToken Manager 삭제 완료

III. KeyToken Manager

KeyToken Manager는 공인인증서의 복사 및 삭제, 그리고 KeyToken의 초기화 및 비밀번호 변경을 위한 KeyToken 관리 소프트웨어입니다.

1. 공인인증서 복사

KeyToken Manager는 공인인증서를 현재의 저장매체에서 다른 저장매체로 복사할 수 있습니다. 하지만 표 1과 같이, 공인인증서를 보안이 매우 취약한 하드 디스크로 복사하는 것은 허용하지 않으며, 또한 한국인터넷진흥원(KISA)의 규격을 준수하여 보안토큰 안의 공인인증서를 다른 저장매체로 복사하는 것도 허용하지 않습니다.

표 1. 공인인증서 복사 가능 저장매체

공인인증서 위치	하드 디스크로 복사하기	이동식 디스크로 복사하기	보안토큰으로 복사하기	백업영역으로 복사하기
하드 디스크	불가능	가능	가능	가능
이동식 디스크	불가능	가능	가능	가능
보안토큰	불가능	불가능	불가능	불가능
백업영역	불가능	가능	가능	불가능

이 절에서는 하드 디스크에 저장되어 있는 공인인증서를 보안토큰과 백업영역으로 복사하는 과정을 예를 들어서 설명합니다. 이동식 디스크 또는 백업영역에 저장되어 있는 공인인증서를 다른 저장매체로 복사하는 과정도 설명할 예와 기본적으로 동일합니다.

[1] 단계는 KeyToken Manager를 실행하는 과정이며, [2] ~ [6] 단계들은 하드 디스크의 공인인증서를 보안토큰으로 복사하는 과정이며, [7] ~ [11] 단계들은 하드 디스크의 공인인증서를 백업영역으로 복사하는 과정입니다. 보안토큰에 저장된 공인인증서는 PC에서 사용할 수 있으며, 백업영역에 저장된 공인인증서는 PC와 NFC 스마트폰에서 사용할 수 있습니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

1 윈도우의 바탕화면에서 그림 25와 같은 'KeyToken Manager' 아이콘을 찾아 더블 클릭하여, KeyToken Manager를 실행시킵니다.

그림 25. KeyToken Manager 아이콘

2 그림 26 화면에서 하드 디스크의 체크박스를 클릭하거나 공인인증서를 더블클릭하여, 복사할 공인인증서를 선택합니다.

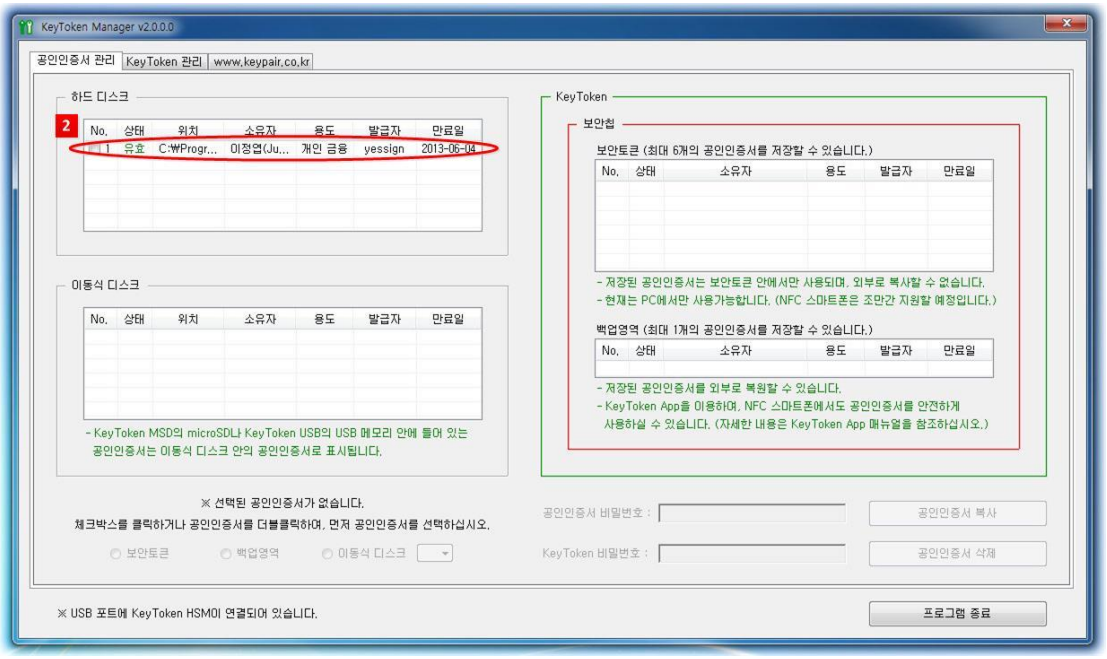

그림 26. 복사할 공인인증서 선택

3 그림 27 화면에서 공인인증서를 복사할 위치인 '보안토큰' 버튼을 선택합니다.

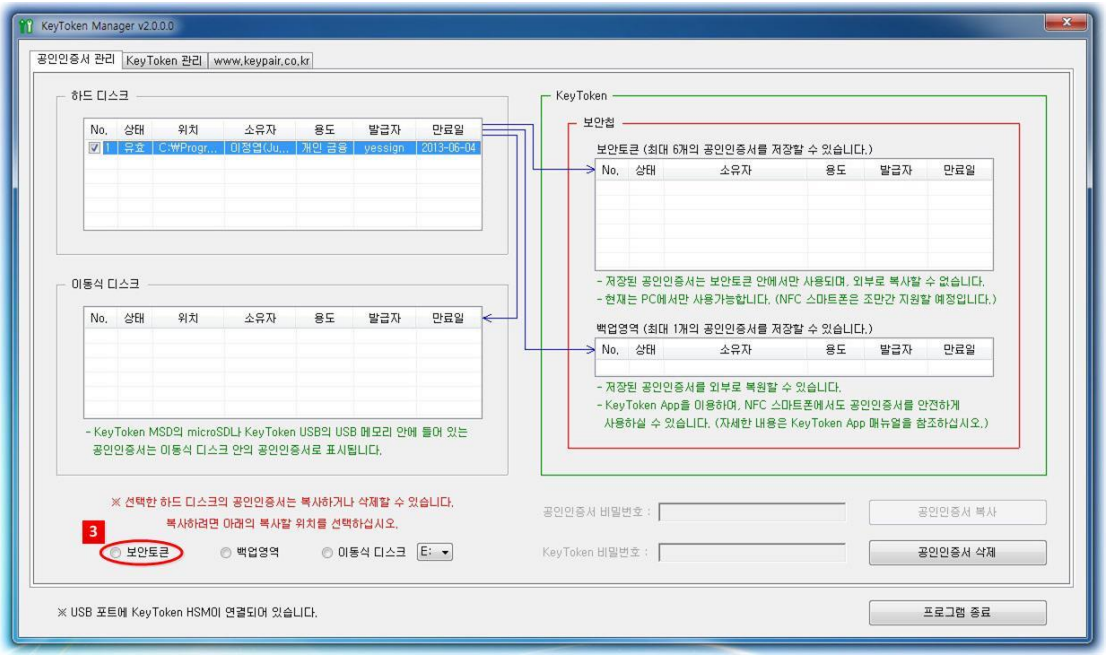

그림 27. 복사할 위치 선택

4 그림 28 화면에서 공인인증서 비밀번호와 KeyToken 비밀번호를 입력합니다.

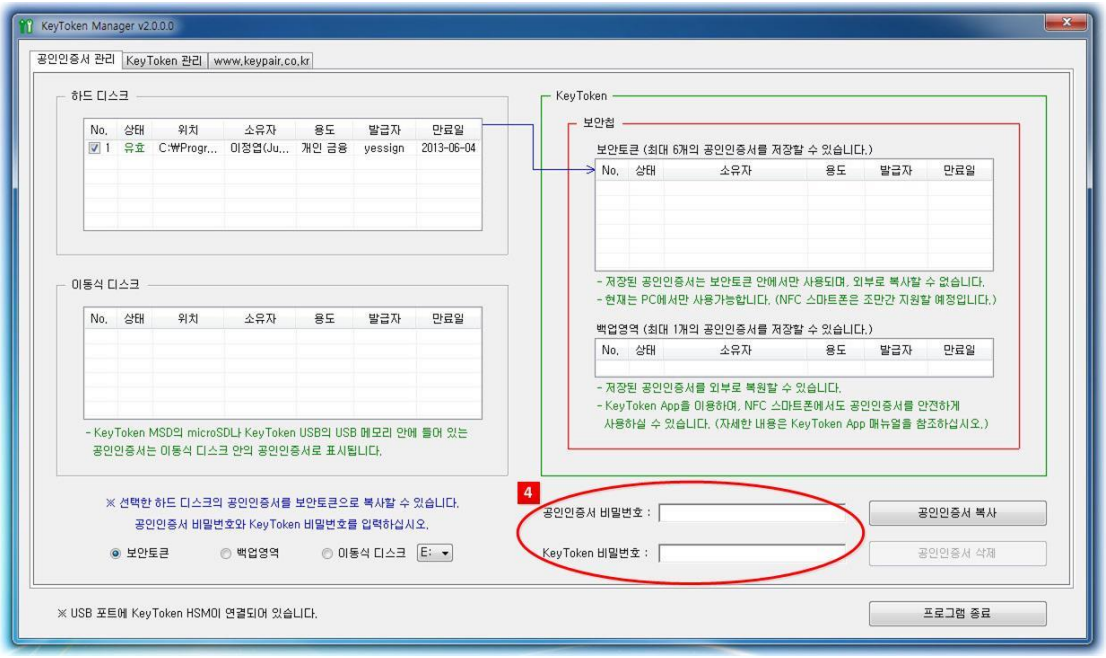

그림 28. 비밀번호 입력

5 그림 29 화면에서 '공인인증서 복사' 버튼을 누릅니다.

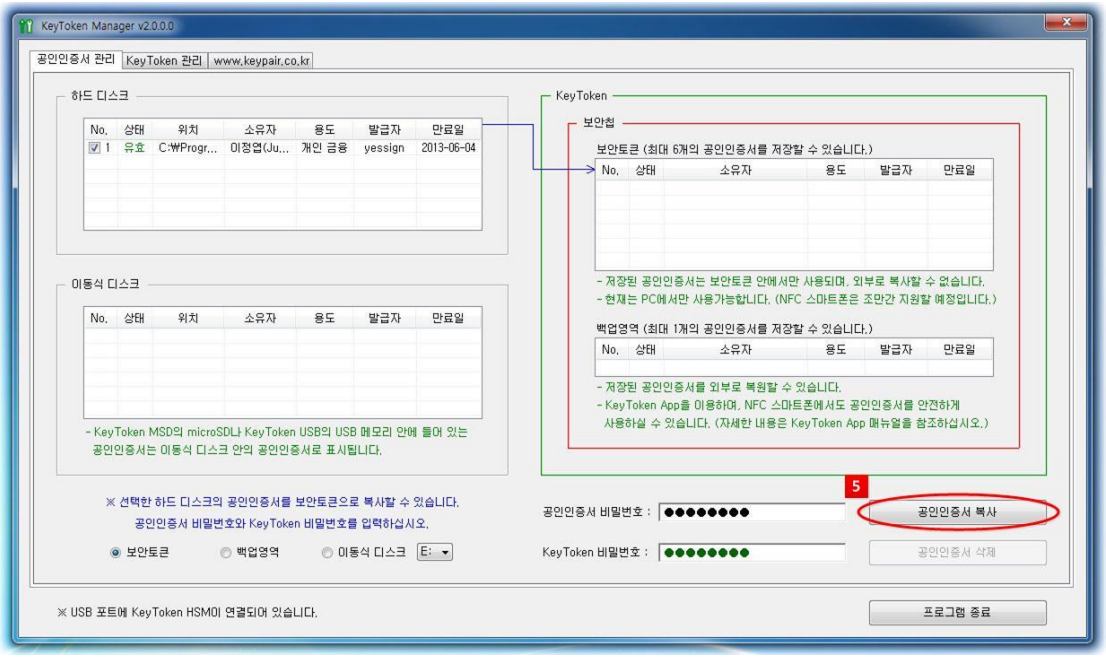

그림 29. 공인인증서 복사

6 그림 30 화면에서 '확인' 버튼을 눌러, 하드 디스크의 공인인증서를 보안토큰으로 복사하는 과정을 완료합니다.

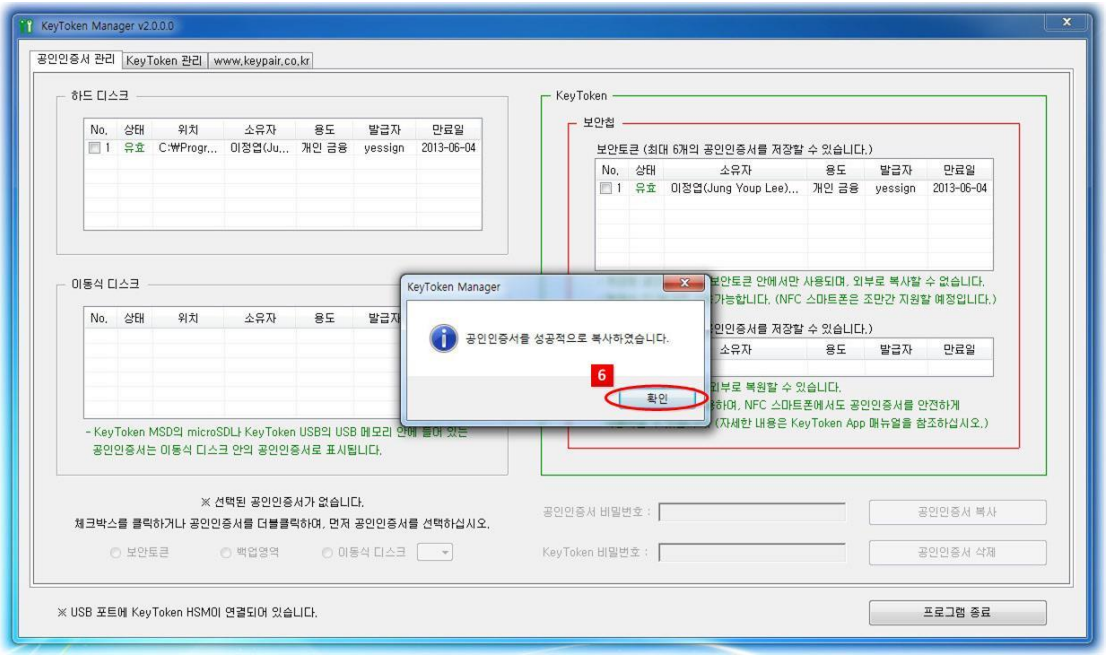

그림 30. 공인인증서 복사 완료

7 그림 31 화면에서 하드 디스크의 체크박스를 클릭하거나 공인인증서를 더블클릭하여, 복사할 공인인증서를 선택합니다.

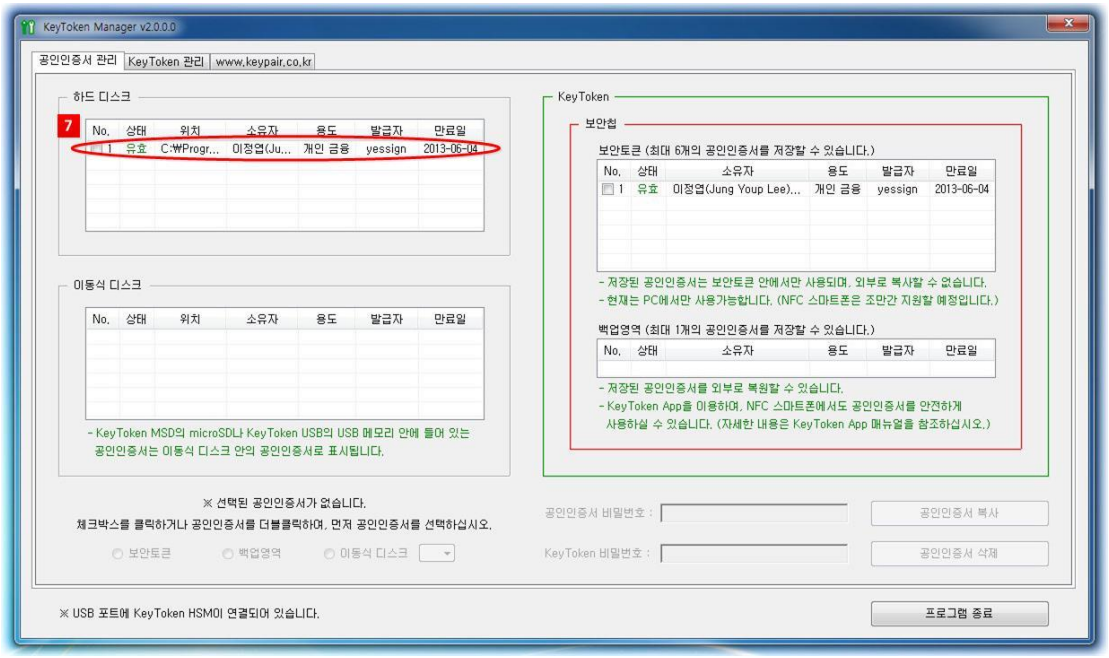

그림 31. 복사할 공인인증서 선택

8 그림 32 화면에서 공인인증서를 복사할 위치인 '백업영역' 버튼을 선택합니다.

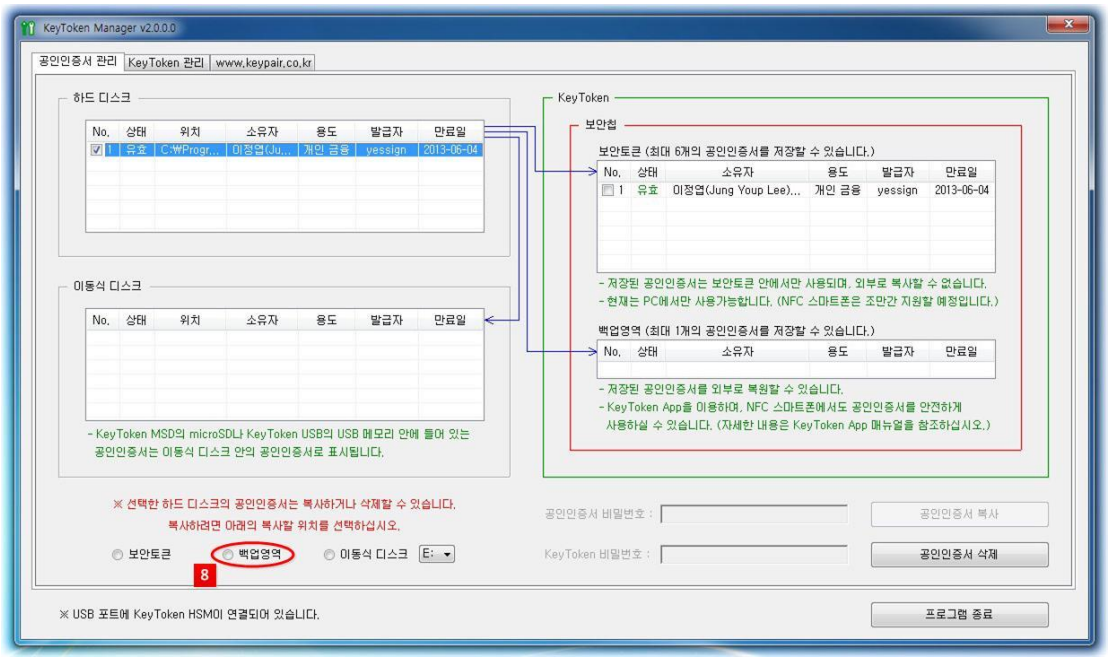

그림 32. 복사할 위치 선택

9 그림 33 화면에서 KeyToken 비밀번호를 입력합니다.

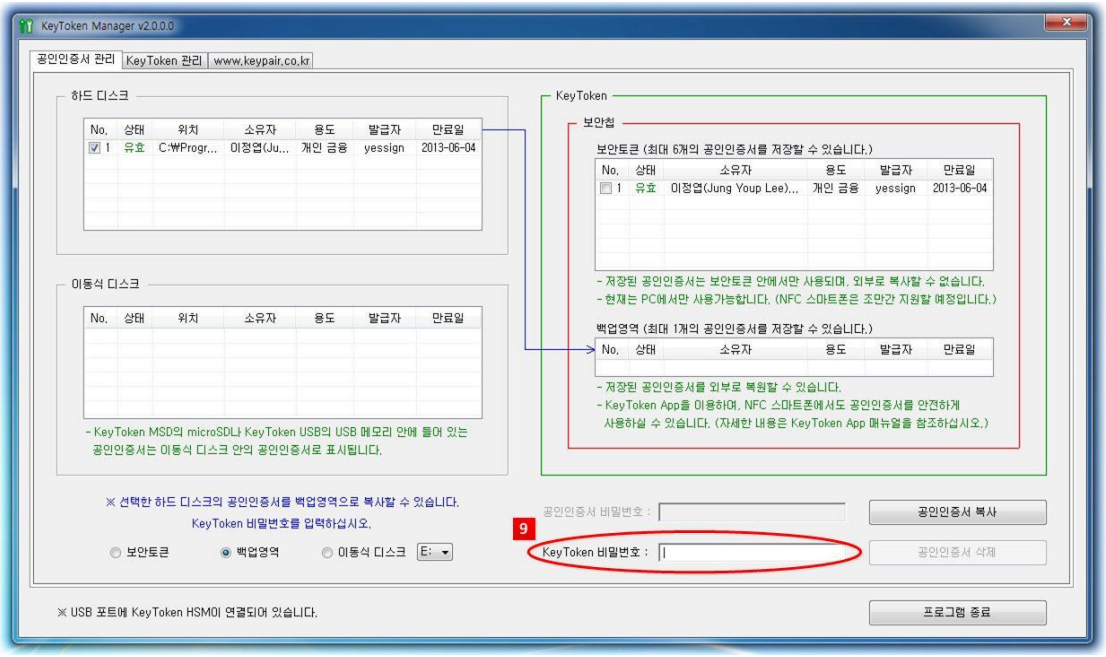

그림 33. 비밀번호 입력

10 그림 34 화면에서 '공인인증서 복사' 버튼을 누릅니다.

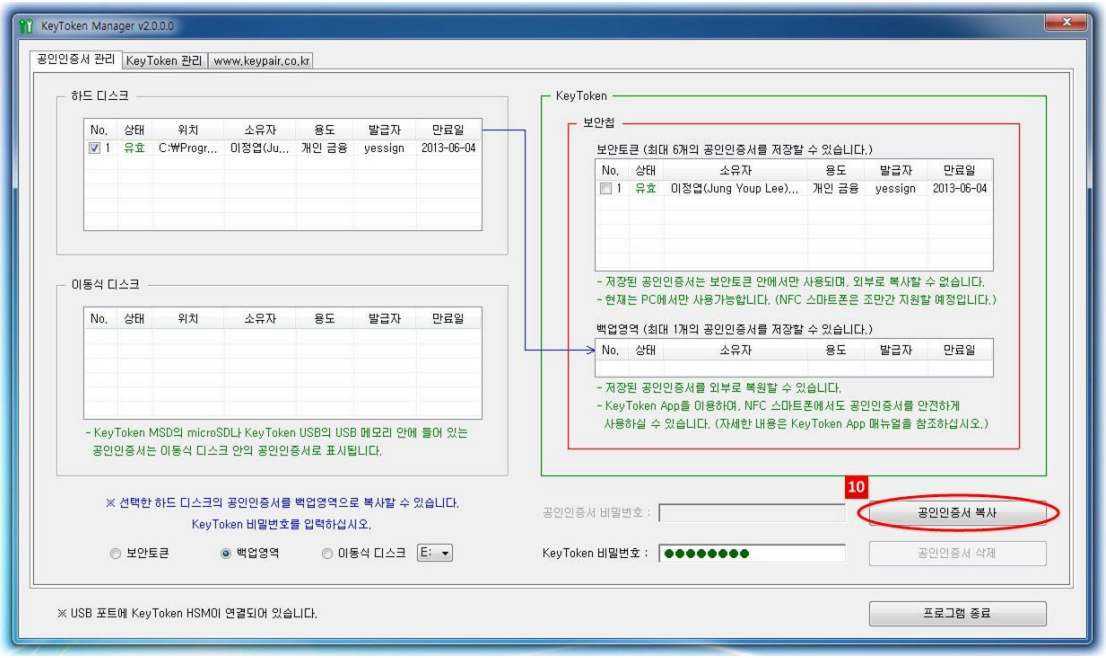

그림 34. 공인인증서 복사

11 그림 35 화면에서 '확인' 버튼을 눌러, 하드 디스크의 공인인증서를 백업영역으로 복사하는 과정을 완료합니다.

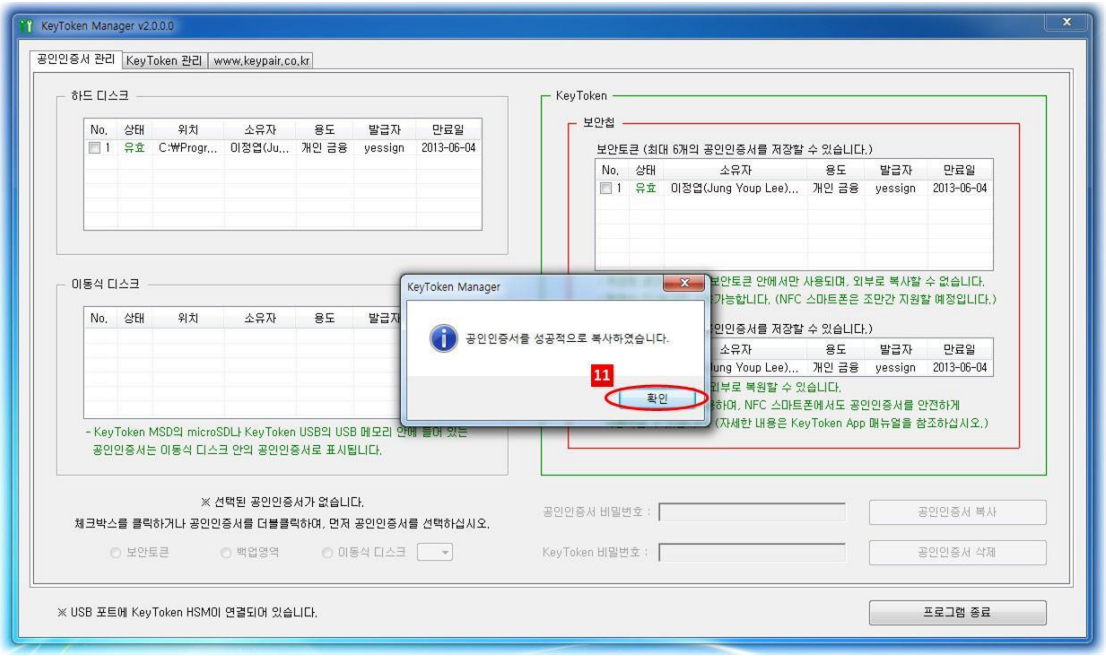

그림 35. 공인인증서 복사 완료

※ 백업영역에 저장된 공인인증서는 그림 36과 같이 KeyToken App을 이용하여 NFC 스마트폰으로 복사할 수 있습니다. 자세한 내용은 'KeyToken App Manual'을 참조하시기 바랍니다.

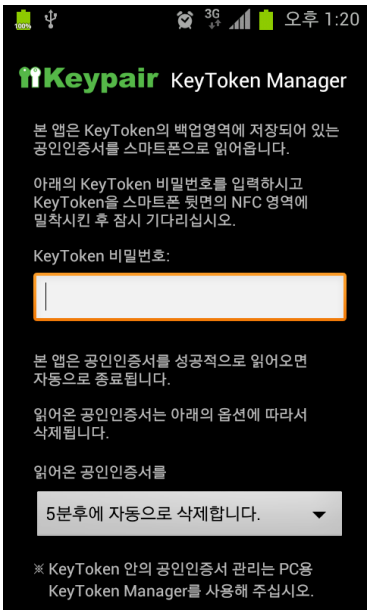

그림 36. KeyToken App 설치 QR 코드 및 실행 화면

2. 공인인증서 삭제

KeyToken Manager는 하드 디스크, 이동식 디스크, 보안토큰, 백업영역에 저장되어 있는 공인인증서를 삭제할 수 있습니다.

이 절에서는 하드 디스크에 저장되어 있는 공인인증서를 삭제하는 과정을 예를 들어서 설명합니다. 이동식 디스크, 보안토큰, 백업영역에 저장되어 있는 공인인증서를 삭제하는 과정도 설명할 예와 기본적으로 동일합니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

1 Ⅲ장 1절의 '공인인증서 복사'에서 [1] 단계를 실행하여, KeyToken Manager를 실행시킵니다.

2 그림 37 화면에서 하드 디스크의 체크박스를 클릭하거나 공인인증서를 더블클릭하여, 삭제할 공인인증서를 선택합니다.

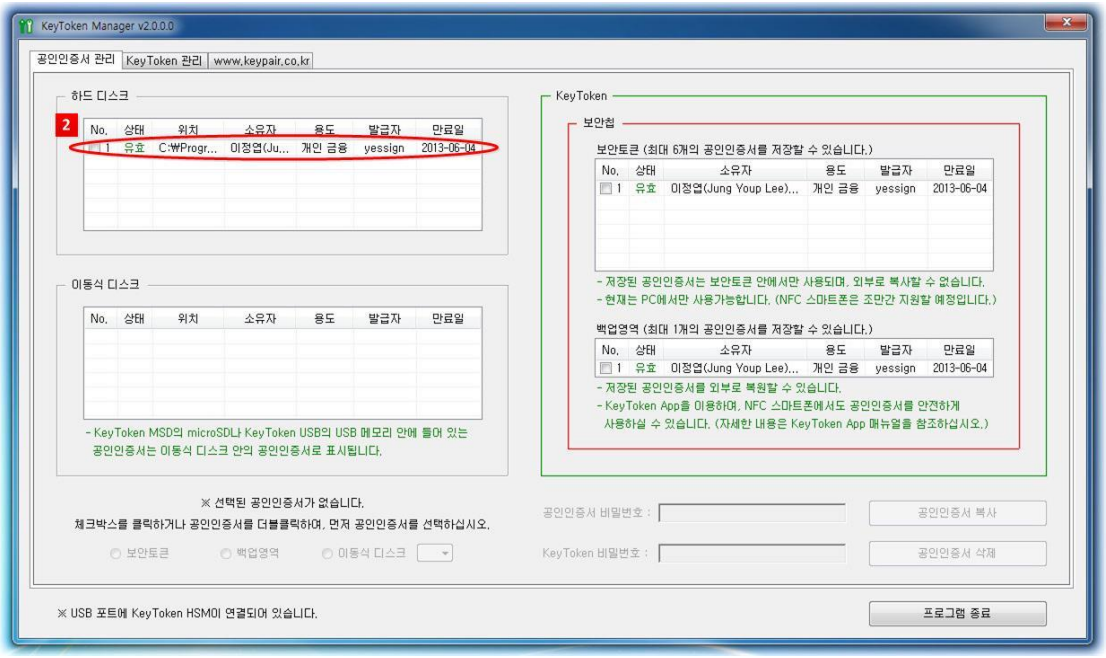

그림 37. 삭제할 공인인증서 선택

3 그림 38 화면에서 '공인인증서 삭제' 버튼을 누릅니다.

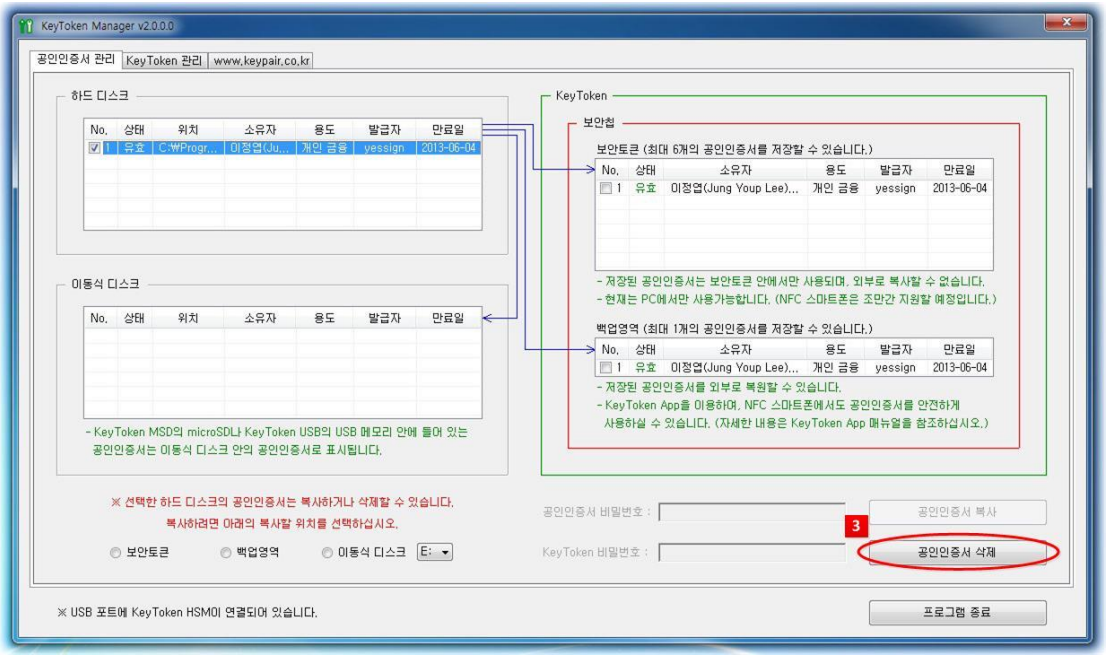

그림 38. 공인인증서 삭제

4 그림 39 화면에서 '예' 버튼을 눌러, 삭제함을 확인합니다.

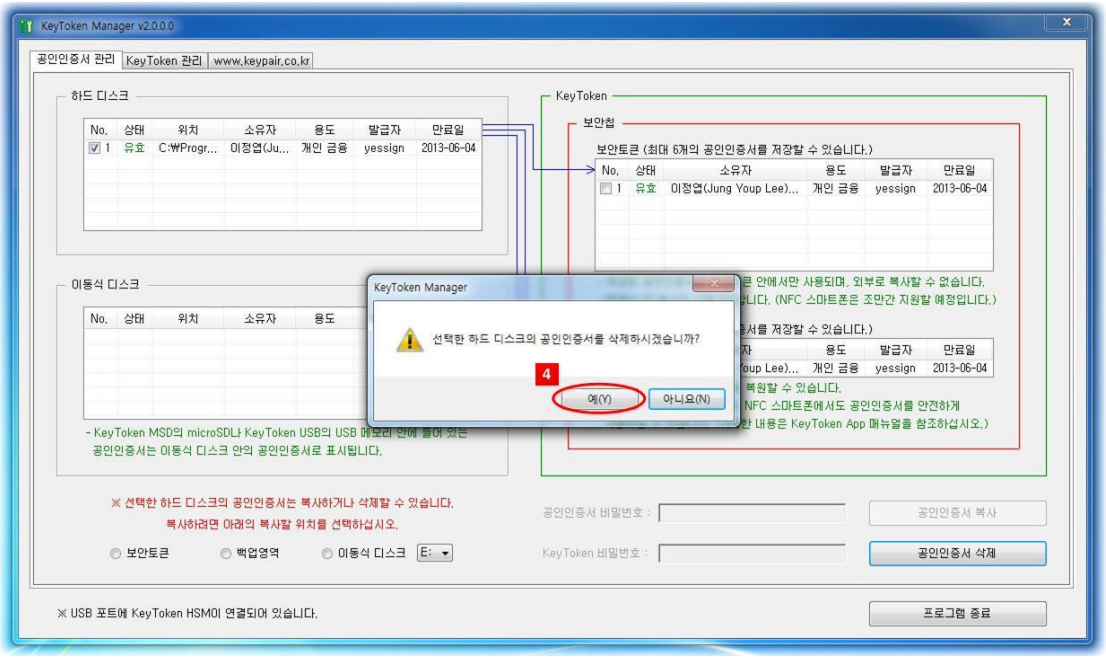

그림 39. 공인인증서 삭제 확인

5 그림 40 화면에서 '예' 버튼을 눌러, 삭제함을 다시 확인합니다.

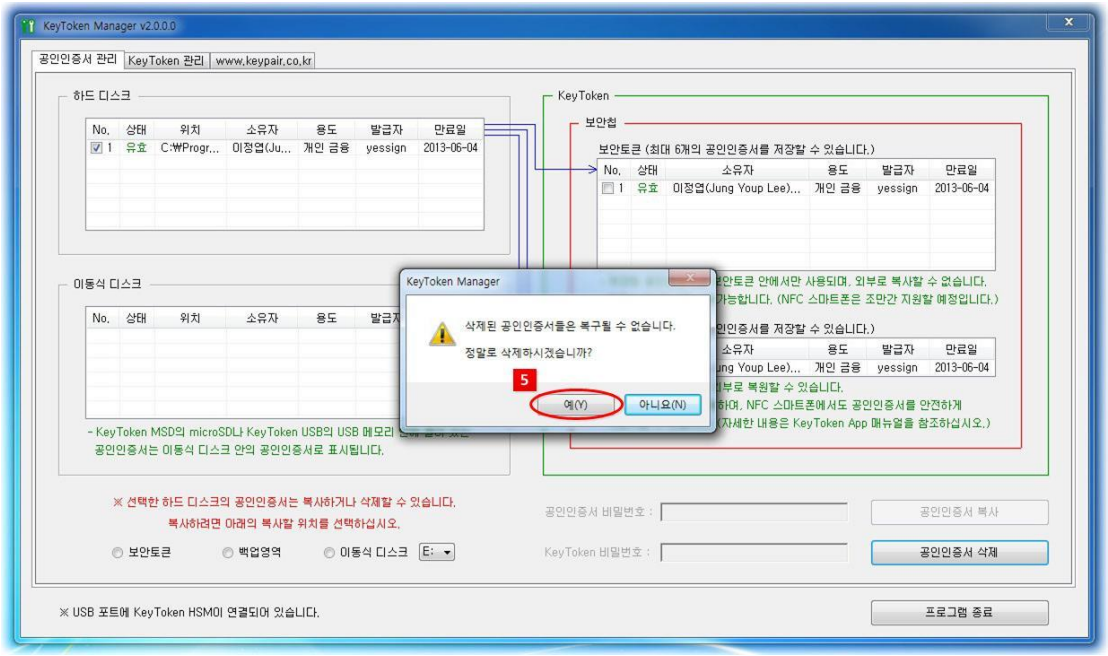

그림 40. 공인인증서 삭제 재확인

6 그림 41 화면에서 '확인' 버튼을 눌러, 하드 디스크의 공인인증서를 삭제하는 과정을 완료합니다.

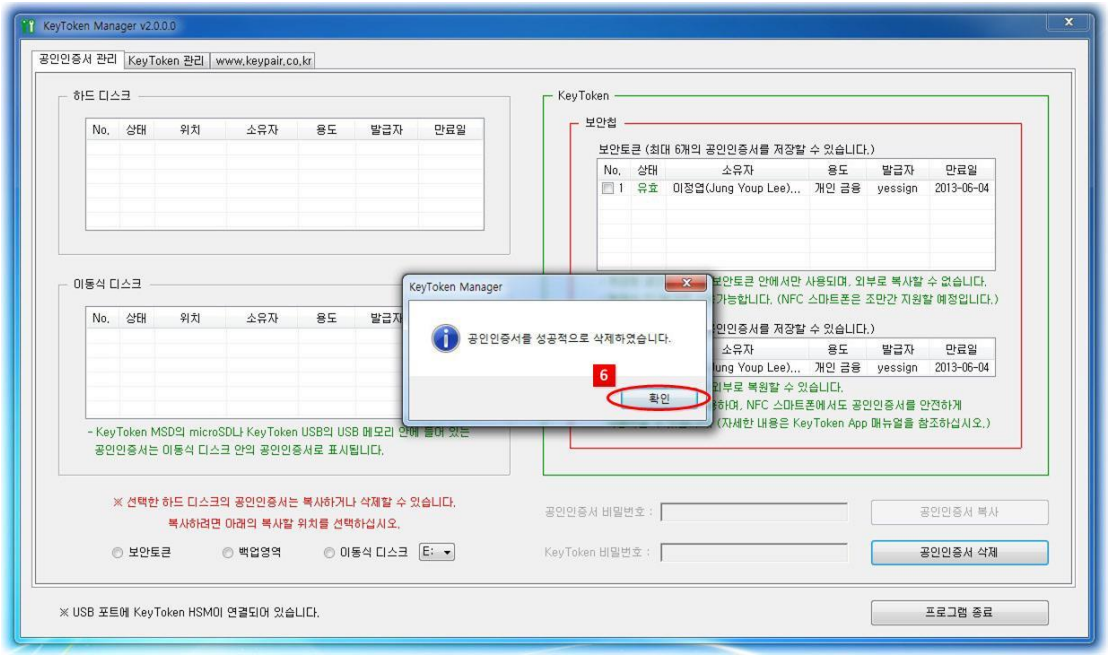

그림 41. 공인인증서 삭제 완료

3. KeyToken 초기화

KeyToken은 정상사용상태이든 잠김상태이든 언제든지 초기화할 수 있습니다. 초기화시 KeyToken 비밀번호와 보안토큰, 백업영역 안의 모든 데이터는 완전히 삭제되므로, KeyToken 비밀번호를 새로 설정해야 하고 공인인증서도 새로 발급받거나 다시 복사해 넣어야 합니다. 하지만, KeyToken MSD의 microSD나 KeyToken USB의 USB 메모리 안의 데이터는 삭제되지 않습니다.

이 절에서는 KeyToken Manager로 KeyToken을 초기화하는 과정을 예를 들어서 설명합니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

1 Ⅲ장 1절의 '공인인증서 복사'에서 [1] 단계를 실행하여, KeyToken Manager를 실행시킵니다.

2 그림 42 화면에서 'KeyToken 관리' 탭을 선택합니다.

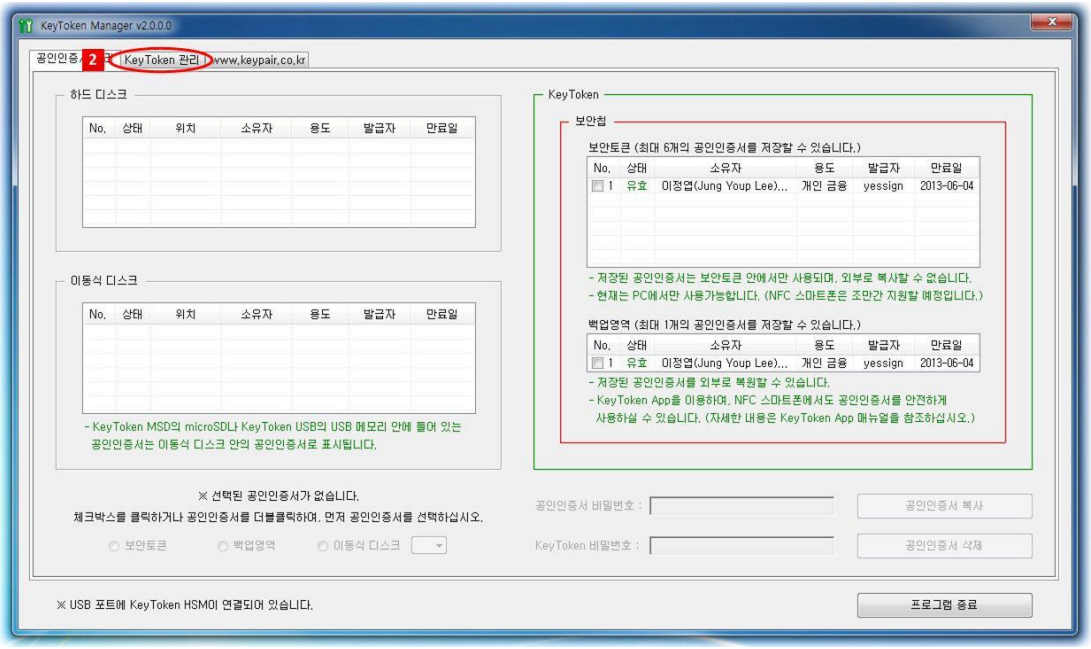

그림 42. KeyToken 관리 탭 선택

3 그림 43 화면에서 KeyToken 비밀번호 등 초기화에 필요한 정보를 입력합니다.

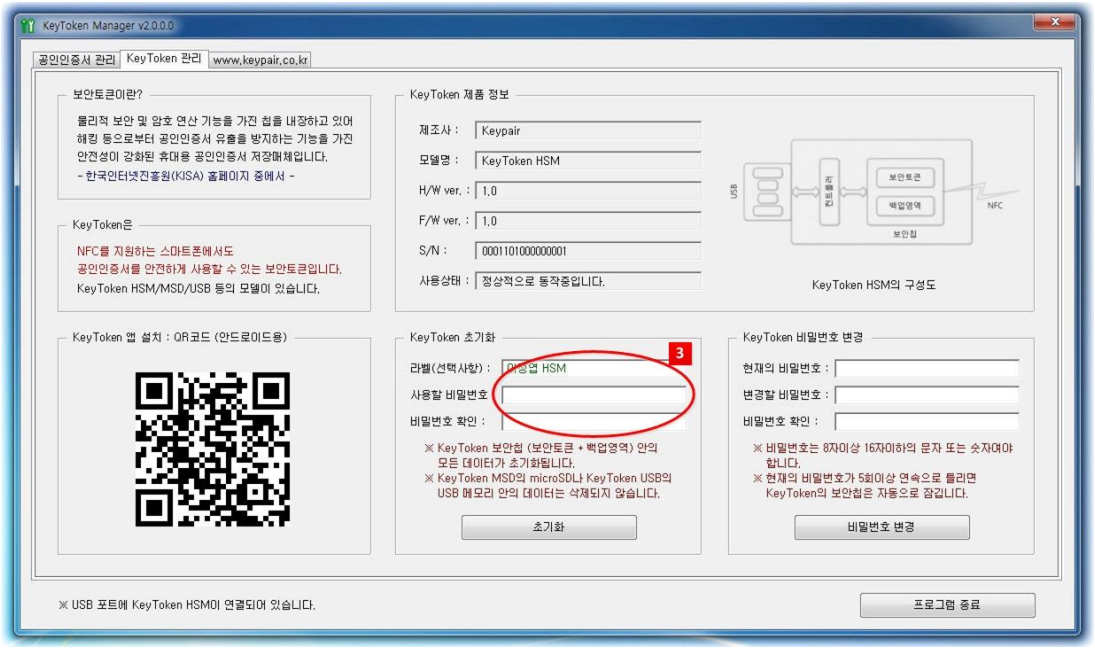

그림 43. KeyToken 초기화 정보 입력

4 그림 44 화면에서 '초기화' 버튼을 누릅니다.

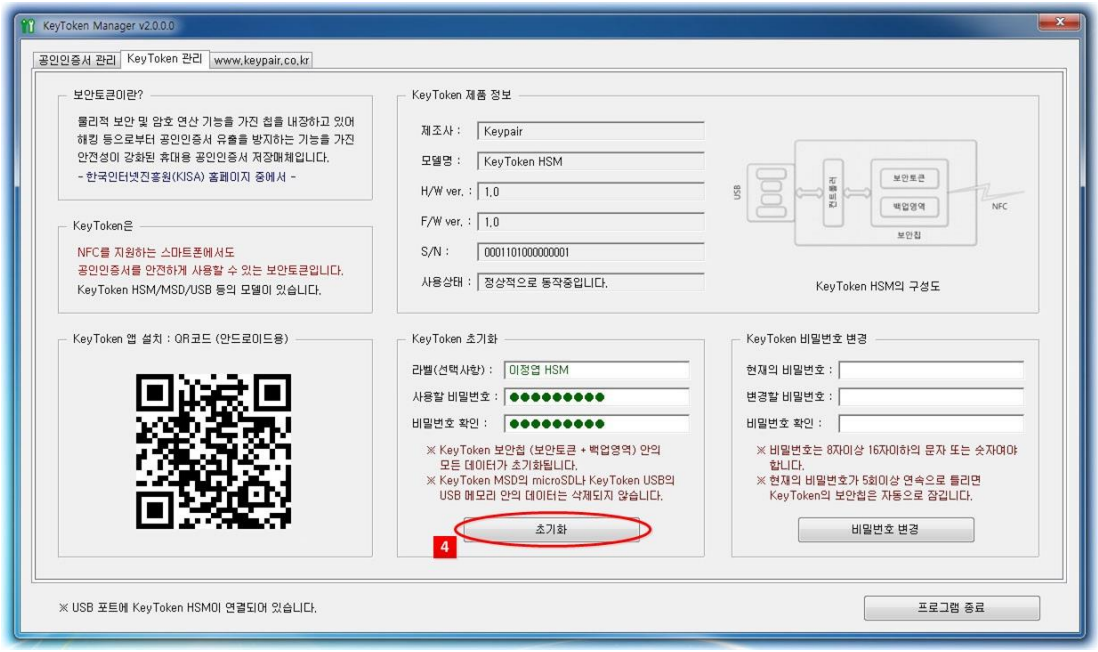

그림 44. KeyToken 초기화 시작

5 그림 45 화면에서 '예' 버튼을 눌러, 초기화함을 확인합니다.

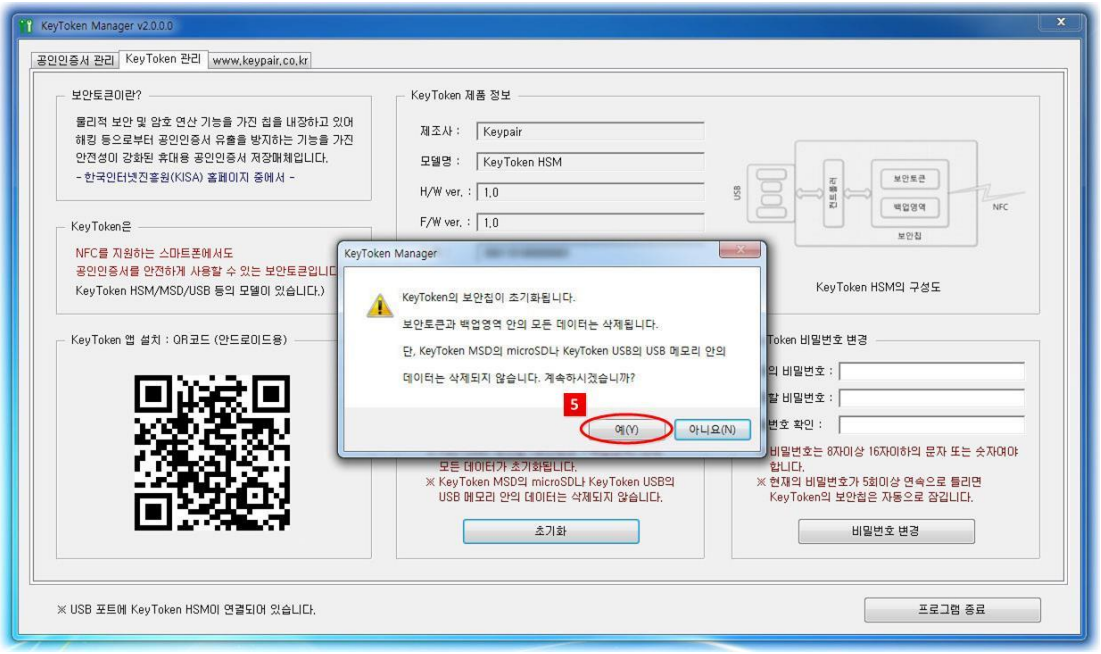

그림 45. KeyToken 초기화 확인

6 그림 46 화면에서 '예' 버튼을 눌러, 초기화함을 다시 확인합니다.

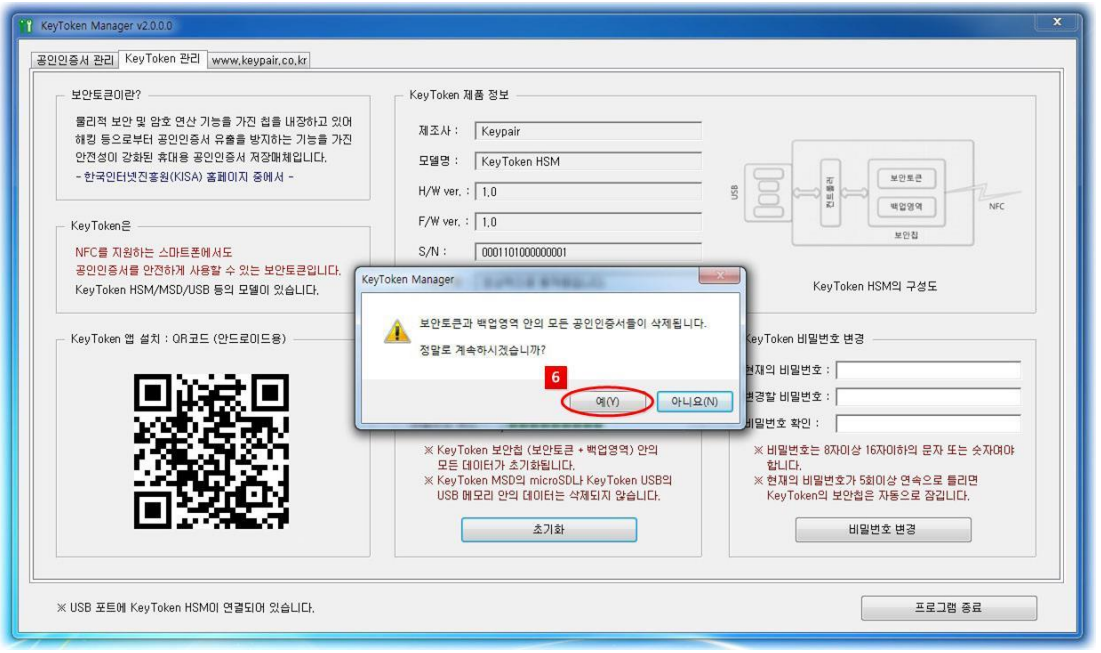

그림 46. KeyToken 초기화 재확인

7 그림 47 화면에서 '확인' 버튼을 눌러, KeyToken 초기화를 완료합니다.

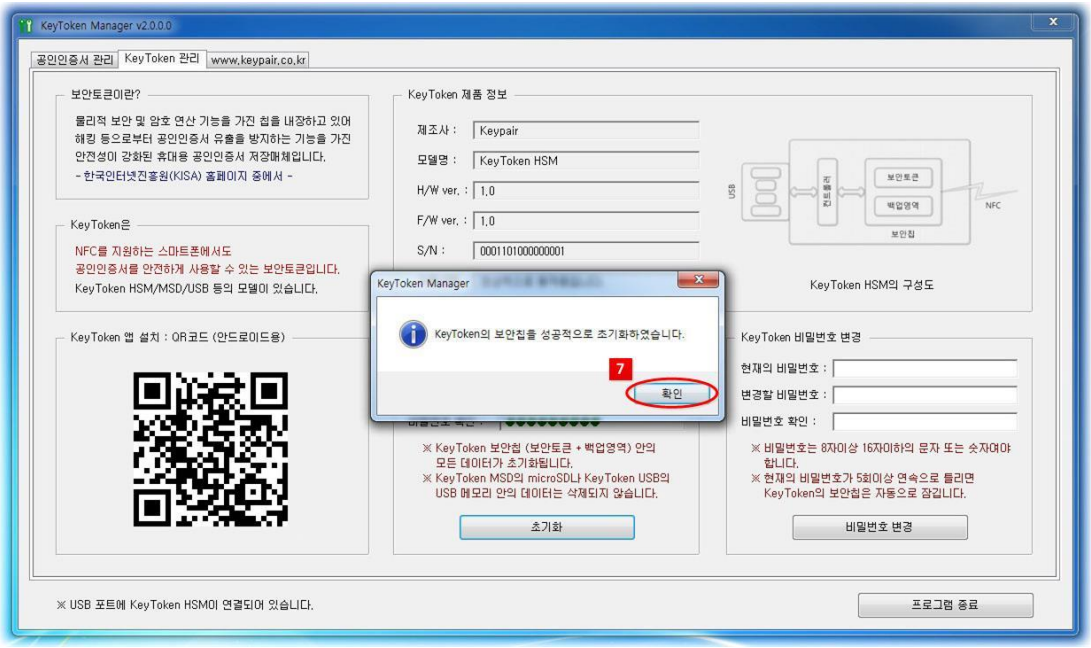

그림 47. KeyToken 초기화 완료

4. KeyToken 비밀번호 변경

보안상 모든 비밀번호는 주기적으로 변경하는 것이 좋습니다. 마찬가지로 KeyToken 비밀번호도 주기적으로 변경할 것을 권장합니다.

이 절에서는 KeyToken Manager로 KeyToken 비밀번호를 변경하는 과정을 예를 들어서 설명합니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

1 III장 3절의 'KeyToken 초기화'에서 [1] 단계를 실행하여, KeyToken Manager를 실행시킵니다.

2 III장 3절의 'KeyToken 초기화'에서 [2] 단계를 실행하여, 'KeyToken 관리' 탭을 선택합니다.

3 그림 48 화면에서 현재의 KeyToken 비밀번호와 변경할 KeyToken 비밀번호를 입력합니다.

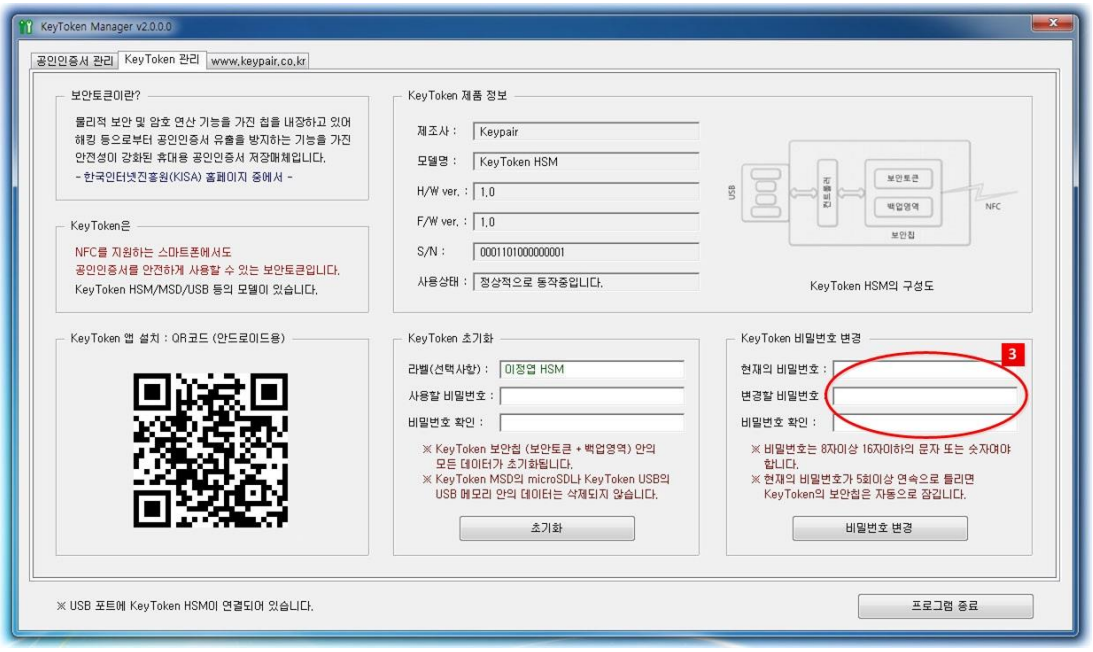

그림 48. KeyToken 비밀번호 입력

4 그림 49 화면에서 '비밀번호 변경' 버튼을 누릅니다.

그림 49. KeyToken 비밀번호 변경 시작

5 그림 50 화면에서 '확인' 버튼을 눌러, KeyToken 비밀번호 변경을 완료합니다.

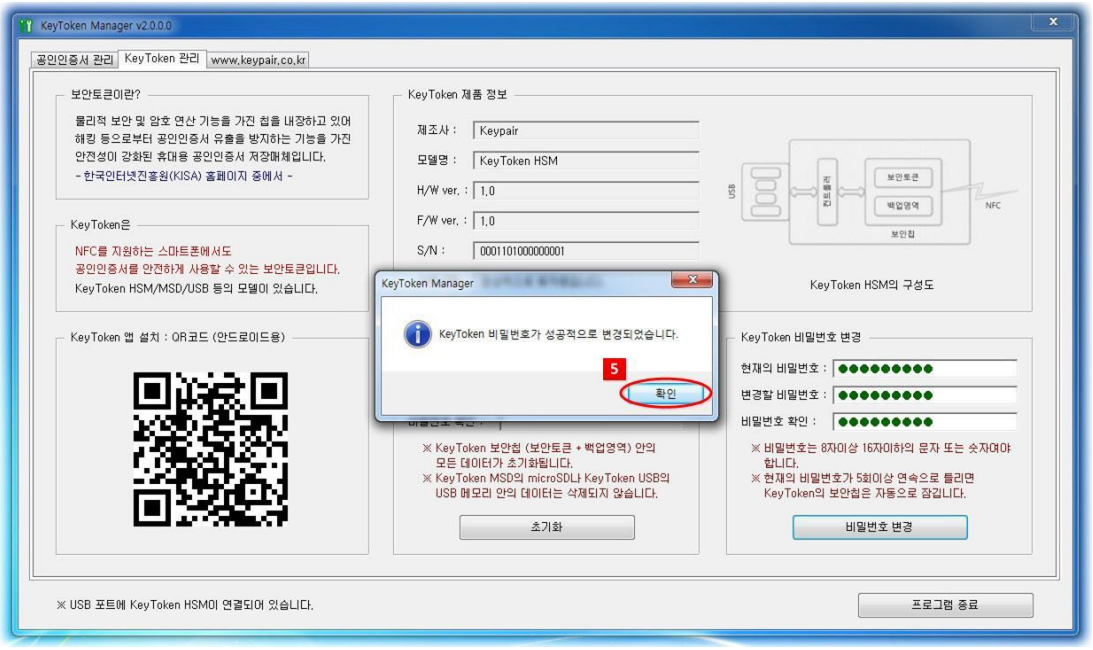

그림 50. KeyToken 비밀번호 변경 완료

5. 키페어 홈페이지 연결

KeyToken Manager에서 'www.keypair.co.kr' 탭을 선택하면, 키페어 홈페이지로 연결됩니다.

그림 51. 키페어 홈페이지 연결

IV. KeyToken 사용하기

KeyToken은 금융 및 공공기관 홈페이지와 연동하여 공인인증서 로그인, 공인인증서 발급, 공인인증서 갱신 등에 사용할 수 있습니다.

1. 공인인증서 로그인

KeyToken으로 금융 및 공공기관 홈페이지에 로그인하는 과정은 기존의 이동식 디스크의 공인인증서로 로그인하는 과정과 거의 동일합니다.

이 절에서는 인터넷뱅킹 가입자가 KeyToken으로 은행 홈페이지에 로그인하는 과정을 예를 들어서 설명합니다. 다른 금융 및 공공기관 홈페이지에서도 아래와 거의 동일한 과정으로 로그인할 수 있습니다.

먼저, PC의 USB 포트에 KeyToken을 연결한 후, 다음의 단계를 시작합니다.

1 그림 52 화면처럼 웹 브라우저 주소창에 은행 홈페이지 주소를 입력하여, 은행 홈페이지에 접속합니다.

2 그림 52 화면에서 '로그인'을 누릅니다.

그림 52. 은행 홈페이지 접속

3 그림 53 화면에서 '보안토큰'을 선택합니다.

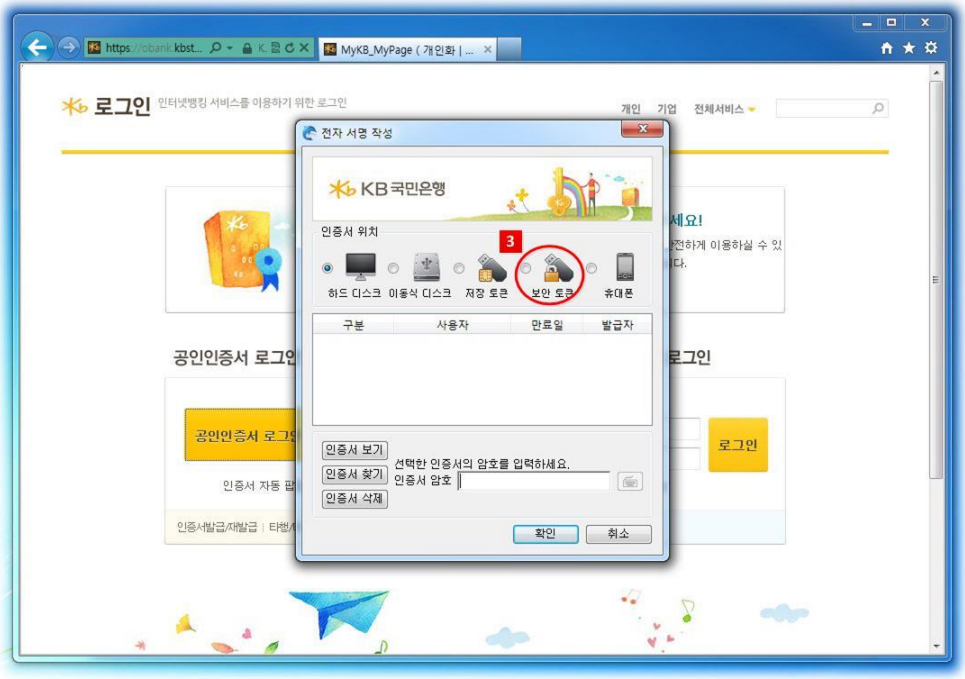

그림 53. 공인인증서 로그인 시작

4 그림 54 화면에서 'Keypair KeyToken: 1.0.0.5'를 선택합니다.

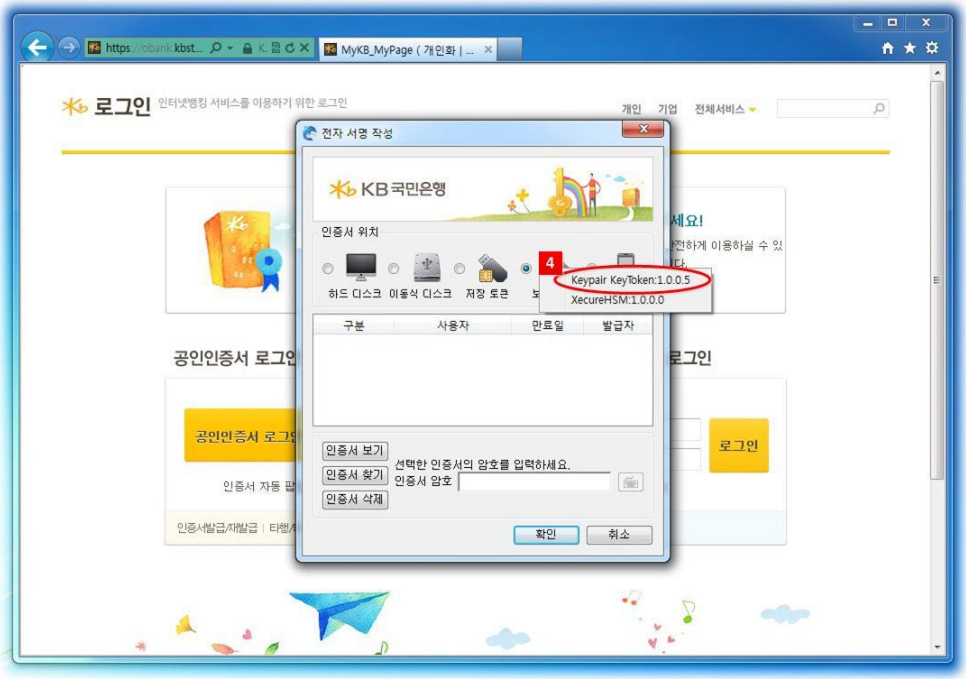

그림 54. KeyToken 선택

5 그림 55 화면에서 KeyToken 비밀번호를 입력합니다.

6 그림 55 화면에서 '확인' 버튼을 눌러, 로그인합니다.

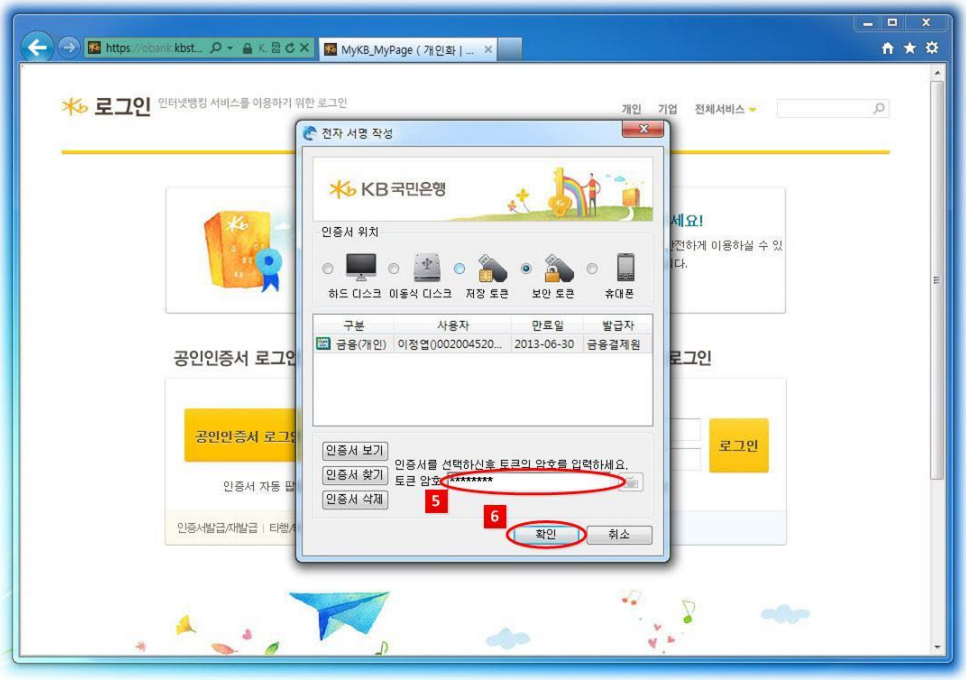

그림 55. KeyToken 비밀번호 입력

7 그림 56 화면처럼 로그인된 화면을 확인합니다.

그림 56. 공인인증서 로그인 완료

※ 증권사 홈페이지에서 KeyToken을 처음으로 사용하는 경우, 그림 57과 같은 화면이 나타날 수 있습니다. 이 화면은 KeyToken을 보안토큰이 아닌 저장토큰으로 사용할 것인지 묻는 것으로 반드시 아래와 같이 '사용안함'으로 설정하셔야 합니다.

1 그림 57 화면에서 '이 저장장치에 대해서 다시 묻지 않음' 체크박스를 체크합니다.

2 그림 57 화면에서 '사용안함'을 누릅니다.

그림 57. 증권사에서 KeyToken 처음으로 사용하기

※ 만약, '사용(OK)'로 설정하였다면, 아래의 과정으로 반드시 '사용안함'으로 변경하시기 바랍니다.

1 그림 58 화면에서 윈도우의 '시작' 버튼을 누릅니다.

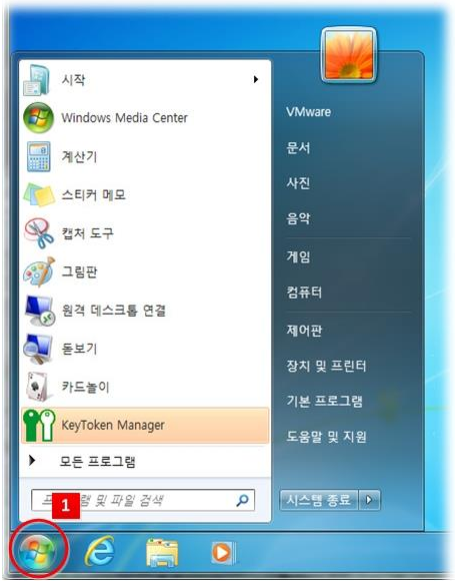

그림 58. 윈도우 시작 버튼 누르기

2 그림 59 화면의 '프로그램 및 파일 검색' 창에 'regedit'를 입력하고, 엔터키를 눌러 실행합니다.

그림 59. regedit 실행하기

3, 4 그림 60 화면처럼 HKEY_CURRENT_USER/Software/AppDataLow/SignKorea/Configuration/pkiclient 밑에 USE_SMARTCARD 항목을 찾습니다.

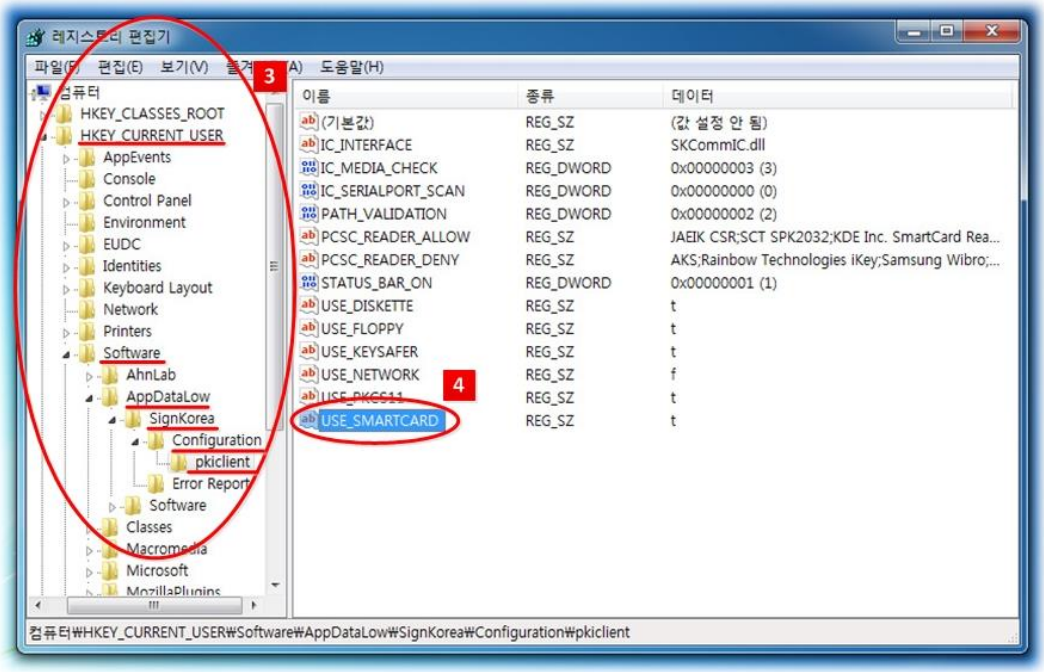

그림 60. USE_SMARTCARD 항목 찾기

5, 6 그림 61 화면에서 값 데이터에 'f'를 입력하고, '확인' 버튼을 누릅니다.

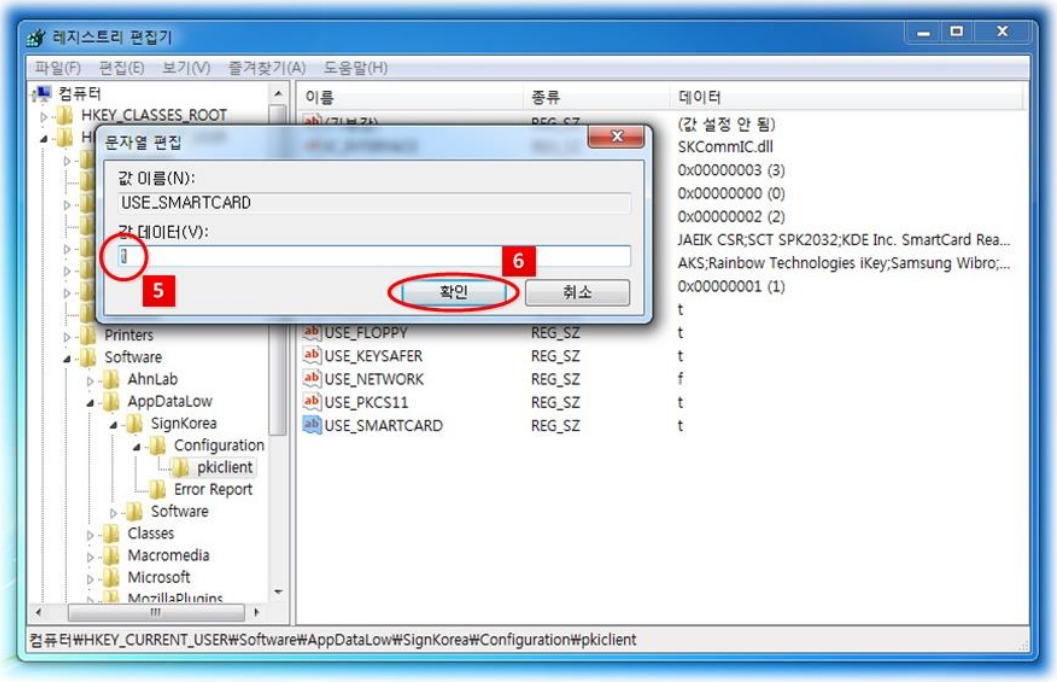

그림 61. USE_SMARTCARD 값 데이터 변경하기

7 그림 62 화면에서 USE_SMARTCARD의 데이터가 'f'로 변경된 것을 확인합니다.

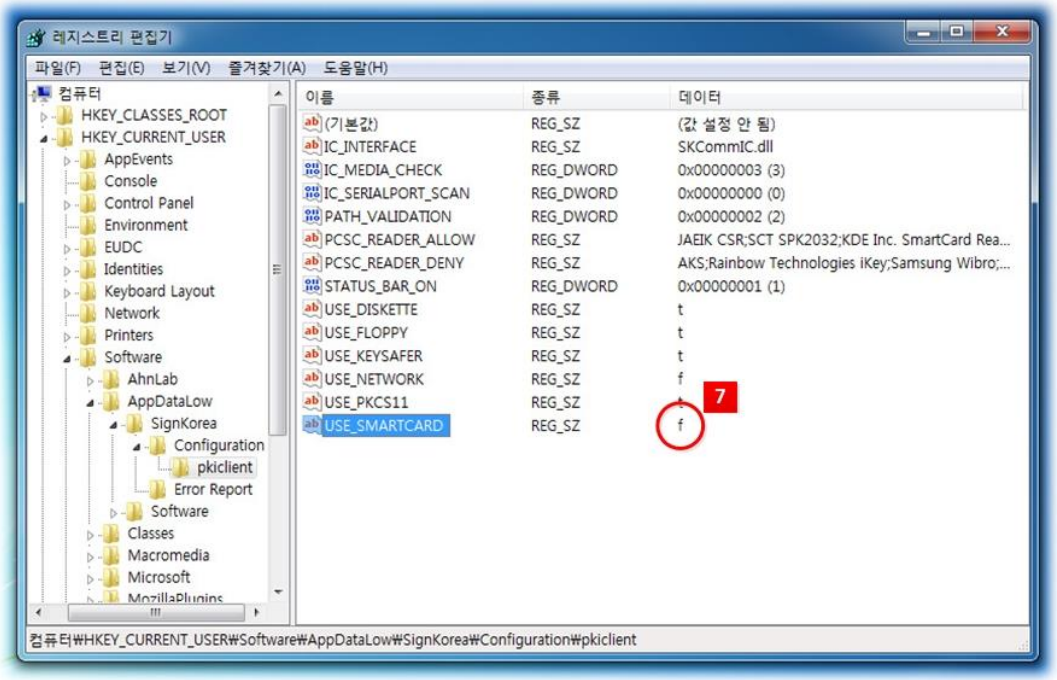

그림 62. USE_SMARTCARD 값 데이터 변경 확인하기

2. 공인인증서 발급

KeyToken은 공인인증서를 안전하게 저장하고 또 안전하게 사용하기 위한 보안토큰으로, 한국인터넷진흥원(KISA)의 구현적합성 평가를 받은 제품입니다.

공인인증서는 이동식 디스크나 하드 디스크 또는 보안토큰으로 발급받을 수 있습니다. 하지만, 이동식 디스크나 하드 디스크로 발급받을 경우, 공인인증서가 파일 형태로 저장되어 쉽게 복사가 가능하기 때문에 해킹에 매우 취약합니다. 그래서, 한국인터넷진흥원(KISA)도 공인인증서를 저장하기 위한 전용 보안 장치인 보안토큰으로 발급받을 것을 권장하고 있습니다.

보안토큰으로 공인인증서를 발급받으면 공인인증서의 외부유출이 원천적으로 방지되어 공인인증서를 가장 안전하게 사용할 수 있습니다.

보안토큰으로 공인인증서를 발급받는 과정은 기존의 이동식 디스크로 공인인증서를 발급받는 과정과 거의 동일하며, 자세한 과정은 거래하시는 금융기관 홈페이지를 참조하시기 바랍니다.

※ 참고로, 보안토큰 안에 저장되어 있는 공인인증서는 이동식 디스크나 하드 디스크로 복사되지 않음에 주의하시기 바랍니다. 가족간에 공인인증서를 공유하는 경우처럼 공인인증서의 복사가 필요한 경우라면, 이동식 디스크로 공인인증서를 발급받은 후, 이동식 디스크의 공인인증서를 보안토큰으로 복사하여 보안토큰을 사용하시고, 공인인증서가 저장되어 있는 이동식 디스크는 사용하지 마시고 안전한 곳에 보관하시기 바랍니다.

3. 공인인증서 갱신

KeyToken은 공인인증서를 안전하게 저장하고 또 안전하게 사용하기 위한 보안토큰으로, 한국인터넷진흥원(KISA)의 구현적합성 평가를 받은 제품입니다.

보안토큰 안에 저장되어 있는 공인인증서를 갱신하는 과정은 기존의 이동식 디스크 안에 저장되어 있는 공인인증서를 갱신하는 과정과 거의 동일하며, 자세한 과정은 거래하시는 금융기관 홈페이지를 참조하시기 바랍니다.

※ 참고로, 보안토큰 안에 저장되어 있는 공인인증서는 이동식 디스크나 하드 디스크로 복사되지 않음에 주의하시기 바랍니다. 만약 원본 공인인증서를 이동식 디스크에 보관하고 있고 사본 공인인증서를 보안토큰 안에서 사용하고 있다면, 반드시 원본 공인인증서를 갱신한 후에 갱신된 원본 공인인증서를 다시 보안토큰으로 복사하여 사용하시기 바랍니다.

V. FAQ

Q. KeyToken이란 무엇인가요?

A. KeyToken은 공인인증서를 안전하게 저장하고 또 안전하게 사용하기 위한 보안토큰으로, 한국인터넷진흥원(KISA)이 KeyToken의 보안토큰에 대한 구현적합성을 평가하고 인증한 제품입니다. PC에서는 USB로 연결하여, 스마트폰에서는 NFC로 연결하여 사용하실 수 있습니다.

Q. KeyToken은 왜 사용해야 하나요?

A. 최근 공인인증서 유출로 인한 금융사고들이 증가하고 있습니다. 하드 디스크에 저장되어 있는 공인인증서는 해킹으로 쉽게 유출될 수 있으며, 이동식 디스크에 저장되어 있는 공인인증서는 이동식 디스크의 분실로 인해 쉽게 유출될 수 있습니다.

KeyToken은 물리적 보안 및 암호연산기능을 가진 보안칩을 내장하여 공인인증서의 외부유출을 원천적으로 방지하며, KeyToken 비밀번호가 연속으로 5회이상 틀리면 KeyToken이 자동으로 잠겨버려 분실시에도 안전합니다. 그래서, 한국인터넷진흥원(KISA)은 보안토큰의 사용을 강력히 권장하고 있습니다.

Q. KeyToken을 사용할 수 있는 곳은 어디인가요?

A. PC 환경에서는 은행, 증권사, 보험사, 신용카드사 등 대부분의 금융기관과 전자민원, 국세청 등 대부분의 공공기관 홈페이지에서 KeyToken을 사용하실 수 있습니다. 다만, 드물게 보안토큰을 지원하지 않는 사이트들이 존재합니다. 이 경우, KeyToken의 백업영역에 보관되어 있는 공인인증서를 이동식 디스크로 복사하여 사용할 수 있습니다.

NFC를 지원하는 스마트폰 환경에서는 아직 KeyToken의 보안토큰 기능은 사용하실 수 없지만, KeyToken의 백업영역 기능을 이용하여 대부분의 금융앱에서 현재의 방식보다 안전하게 공인인증서를 사용하실 수 있습니다. 자세한 내용은 'KeyToken App Manual'을 참조하시기 바랍니다.

Q. 이동식 디스크에서 사용하던 공인인증서를 KeyToken에서도 사용할 수 있나요?

A. 네, 사용하실 수 있습니다. 이동식 디스크에 저장되어 있는 공인인증서를 KeyToken으로 복사하여 사용하시면 됩니다.

Q. 공인인증서를 KeyToken에 저장했는데, 다른 매체로 복사할 수 없나요?

A. KeyToken은 보안토큰 기능과 백업영역 기능이 있습니다. KeyToken의 보안토큰에 저장되어 있는 공인인증서는 다른 매체로 복사하실 수 없습니다. 하지만, KeyToken의 백업영역에 보관되어 있는 공인인증서는 다른 매체로 복사하실 수 있습니다.

Q. KeyToken 비밀번호를 잊어버렸습니다. 어떻게 해야 하나요?

A. 죄송합니다만, 현재 KeyToken의 보안토큰과 백업영역 안에 저장되어 있는 공인인증서들은 더 이상 사용하실 수 없습니다. KeyToken 비밀번호가 연속으로 5회이상 틀리면 KeyToken은 자동으로 잠겨버립니다. KeyToken을 초기화하시고, 공인인증서를 새로 발급받으시거나 다시 복사해 넣으셔야 합니다.

Q. KeyToken 구동 프로그램을 다운로드 받아 실행하려고 하는 데, "KeyTokenSetup.exe은(는) 일반적으로 다운로드되는 파일이 아니며, 컴퓨터를 손상시킬 수 있습니다."는 경고 메시지가 나옵니다. 어떻게 해야 하나요?

A. Internet Explorer 9 이상에서 SmartScreen 필터가 활성화되어 있는 경우, 위의 경고 메시지가 나타날 수 있습니다. 이는 마이크로소프트사의 SmartScreen 필터의 정책인 '해당 프로그램을 상당한 수의 다른 Internet Explorer 사용자가 다운로드한 프로그램 목록'에 없기 때문으로, 걱정하지 마시고 설치하시면 됩니다.

Q. KeyToken을 PC의 USB 포트에 연결하였는 데, "장치 드라이버 소프트웨어가 제대로 설치되지 않았습니다."는 경고 메시지가 나옵니다. 어떻게 해야 하나요?

A. KeyToken 구동 프로그램이 정상적으로 설치되지 않은 경우, 위의 경고 메시지가 나올 수 있습니다. KeyToken 구동 프로그램을 다시 설치하시기 바랍니다.

[Blank Page]